

MAKING PATIENT PRIVACY A REALITY: DOES THE FINAL HHS REGULATION GET THE JOB DONE?

HEARING

OF THE

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ON

EXAMINING THE EFFECTIVENESS OF THE NEW DEPARTMENT OF
HEALTH AND HUMAN SERVICES' REGULATIONS THAT MAINTAIN THE
PRIVACY OF PERSONAL HEALTH INFORMATION IN THE FACE OF AD-
VANCED INFORMATION TECHNOLOGY AND THE INCREASING NUMBER
OF ACCESS TO IDENTIFIABLE HEALTH INFORMATION

FEBRUARY 8, 2001

Printed for the use of the Committee on Health, Education, Labor, and Pensions



U.S. GOVERNMENT PRINTING OFFICE

70-383 CC

WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office

Internet: bookstore.gpo.gov Phone: (202) 512-1800 Fax: (202) 512-2250

Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

JAMES M. JEFFORDS, Vermont, *Chairman*

JUDD GREGG, New Hampshire

BILL FRIST, Tennessee

MICHAEL B. ENZI, Wyoming

TIM HUTCHINSON, Arkansas

JOHN W. WARNER, Virginia

CHRISTOPHER S. BOND, Missouri

PAT ROBERTS, Kansas

SUSAN M. COLLINS, Maine

JEFF SESSIONS, Alabama

EDWARD M. KENNEDY, Massachusetts

CHRISTOPHER J. DODD, Connecticut

TOM HARKIN, Iowa

BARBARA A. MIKULSKI, Maryland

JEFF BINGAMAN, New Mexico

PAUL D. WELLSTONE, Minnesota

PATTY MURRAY, Washington

JACK REED, Rhode Island

JOHN EDWARDS, North Carolina

HILLARY RODHAM CLINTON, New York

MARK E. POWDEN, *Staff Director*

J. MICHAEL MYERS, *Minority Staff Director and Chief Counsel*

(II)

CMS Library
C2-07-13
7500 Security Blvd.
Baltimore, Maryland 21244

C O N T E N T S

STATEMENTS

THURSDAY, FEBRUARY 8, 2001

	Page
Jeffords, Hon. James M., Chairman, Committee on Health, Education, Labor, and Pensions, opening statement	1
Kennedy, Hon. Edward M., a U.S. Senator from the State of Massachusetts, opening statement	2
Aronovitz, Leslie G., Director, Health Care, Program Administration and Integrity Issues, U.S. General Accounting Office, Chicago, IL	4
Prepared statement	6
Dodd, Hon. Christopher J., a U.S. Senator from the State of Connecticut, prepared statement	18
Harkin, Hon. Tom, a U.S. Senator from the State of Iowa, prepared statement	25
Wellstone, Hon. Paul D., a U.S. Senator from the State of Minnesota, prepared statement	30
Goldman, Janlori, director, health privacy project, Institute for Healthcare Research and Policy, Georgetown University, Washington, DC; Jane F. Greenman, deputy general counsel for human resources, Honeywell International, Inc., Morristown, NJ, on behalf of the American Benefits Counsel; and John P. Houston, director, production services, data security officer, and assistant counsel, UPMC Health System, Pittsburgh, PA, on behalf of the American Hospital Association	33
Prepared statements of:	
Ms. Goldman	38
Ms. Greenman	42
Mr. Houston	49
Lichtman, Judith L., president, the National Partnership for Women and Families, Washington, DC; Dr. G. Richard Smith, Jr., director, Centers for Mental Healthcare Research, University of Arkansas for Medical Sciences, Little Rock, AR, on behalf of the Association of American Medical Colleges; and Robert C. Heird, senior vice president, Anthem Blue Cross and Blue Shield, Indianapolis, IN, on behalf of Blue Cross/Blue Shield Association	59
Prepared statements of:	
Ms. Lichtman	60
Dr. Smith	68
Mr. Heird	76
Frist, Hon. Bill, a U.S. Senator from the State of Tennessee, prepared statement	86
American Council of Life Insurers, prepared statement	87
American Psychiatric Association, prepared statement	91
Bazelon, Judge David L., Center for Mental Health Law, prepared statement	94
National Association of Chain Drug Stores, prepared statement	101
American Psychoanalytical Association, prepared statement	104
Healthcare Leadership Council, prepared statement	107
Association for Healthcare Philanthropy, prepared statement (with attachments)	109
Health Privacy Project, prepared statement	118

ADDITIONAL MATERIAL

Articles, publications, letters, etc.:	
Thirty-nine organizations letter to Secretary Thompson concerning issued regulations, dated February 7, 2001	36

IV

	Page
Thirty-six organizations submitted on behalf of the Mental Health Liaison Group to Senator Jeffords	96
Tommy G. Thompson, Secretary, Department of Health and Human Services, from Alan F. Holmer, president, Pharmaceutical Research and Manufacturers of America, dated February 13, 2001	98

MAKING PATIENT PRIVACY A REALITY: DOES THE FINAL HHS REGULATION GET THE JOB DONE?

THURSDAY, FEBRUARY 8, 2001

U.S. SENATE,
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS,
Washington, DC.

The committee met, pursuant to notice, at 9:33 a.m., in room SD-430, Dirksen Senate Office Building, Hon. James M. Jeffords (chairman of the committee) presiding.

Present: Senators Jeffords, Frist, Hutchinson, Collins, Roberts, Kennedy, Dodd, Harkin, Bingaman, Wellstone, Murray, Reed, and Clinton.

OPENING STATEMENT OF SENATOR JEFFORDS

The CHAIRMAN. The HELP Committee will come to order.

Good morning. This marks the Health and Education Committee's ninth hearing on one of the most pressing issues confronting our health care system—the confidentiality of our medical information.

We live in an era where major advances in information technology have the potential to improve the quality of our Nation's health care system tremendously. Technology has provided the tools to allow ease of access to an abundance of health care information.

However, quality care requires more than the free flow of information between providers, payers, and other users of health information. It requires trust between a patient and a caregiver. For our health care system to be effective as well as efficient, patients must feel comfortable revealing sensitive personal information to health professionals. Thus, new protections are needed to ensure the confidentiality of this personal health information.

We worked hard in the last Congress to develop a bipartisan approach to medical privacy, but some issues unfortunately remained unresolved. Therefore, in the absence of congressional action, the Secretary of Health and Human Services issued final regulations on December 20, 2000, entitled, "Standards for Privacy of Individually Identifiable Health Information."

To more fully appreciate the significance of this final regulation in relation to the quality of our Nation's health care system, I asked the GAO to conduct interviews with organizations representing patients, health care providers, employers, insurance companies, and research organizations.

At today's oversight hearing, the GAO testimony will focus on the rights of patients and the responsibilities of entities that use patients' personal health information, as set forth in the HHS regulation.

We will also hear from witnesses who will discuss the concerns of key stakeholders regarding the regulation's major provisions.

This hearing will provide the committee with valuable information regarding the final regulation, as well as an evaluation of the need for additional legislative action to ensure that Americans' personal health information is protected.

The hearing will follow the committee's usual format. Each of the witnesses will speak for 5 minutes, and each member will have up to 5 minutes per round for questioning. The hearing record will remain open for 2 weeks, and any written statements and questions for the record should be submitted within that time frame.

That said, let me welcome all of our witnesses. I look forward to hearing your testimony.

I will now turn to my good friend, Senator Kennedy, for his opening comments.

OPENING STATEMENT OF SENATOR KENNEDY

Senator KENNEDY. Thank you very much, Mr. Chairman, for holding this hearing on the confidentiality of patients' medical records and information.

The Health Insurance Portability and Accountability Act of 1996 was developed and reported out of this committee, and we spent a great deal of time on this issue in the last Congress. Although we failed to report out a privacy bill, the committee's action paved the way for the privacy regulations under consideration today. So the protections in the regulations will provide all Americans with control over their medical information and peace of mind that their personal health information will not be used for unauthorized purposes.

The Department of Health and Human Services deserves great credit for its work on this rule, and the Department considered more than 50,000 comments from interested parties. It is not a partisan issue, and I am hopeful that the new administration will support it.

Clearly, the standards and procedures in the regulation present new challenges for the health care system. As we know, the dot-com era enables personal health information to be transmitted with the click of a mouse. We cannot ignore the profound consequences that occur if such information is abused.

Some will express concern that these regulations are burdensome. But, it is a far greater burden to have to look for work because your medical information was shared with your employer, who then fired you.

Many other potential abuses could easily be cited and could easily be prevented by appropriate regulations.

Medical professionals, researchers, and insurance companies have legitimate interests in medical records and health information, but effective privacy protections are needed to protect that information from being obtained by employers, sales agents, or even neighbors. It is not too much to ask that access to such sensitive

information must be limited and subject to authorization, except in rare circumstances.

The current regulation is a significant step in providing needed protection. But, the Secretary's authority was limited, and further steps are needed to meet the challenges of the information age. The statute did not allow the Secretary to establish new rights for legal remedies when confidentiality is violated. Experience shows that a private right of action is an effective deterrent against violations. Often, it is the only way to provide adequate compensation when deterrence fails.

Many of us feel that access to medical records should be at least as limited as access to video rental records. Current law requires law enforcement officers seeking video rental records to obtain a warrant, but this regulation does not provide a similarly high standard for law enforcement access to health information.

In addition, the statute specifically limited the application of the regulation to just a few holders and users of health information. We need to broaden the scope of those covered by these important protections. Many important State laws offer additional protections.

All Americans deserve the peace of mind that comes with knowing that their private medical information remains just that—private.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Hutchinson has a conflict later on, and he has a witness who will be appearing on the third panel whom he would like to say some kind words about.

Senator HUTCHINSON. Indeed. Thank you, Mr. Chairman. Thank you for calling this hearing.

I think the fact that this is the ninth hearing on this subject is reflective of how important this topic is. So I commend you for doing that, and I apologize—the Armed Services Committee is meeting simultaneously with an important hearing with the Secretary of Energy, so I am going to have to excuse myself.

But we are very privileged on one of our later panels to have as a witness today Dr. Richard Smith, who is a graduate of the University of Arkansas College of Medicine and currently the interim chairman of the department of psychiatry and behavioral sciences at the University of Arkansas for Medical Sciences. He is well-known for his extensive research in the area of mental health services, and his testimony today regarding the impact of the Department's privacy regulations will be extremely helpful to this committee as it seeks to understand the impact of these regulations on teaching and medical colleges across the country.

As you have pointed out, Mr. Chairman, unless these regulations are carefully crafted, they have the potential of bringing to a grinding halt the advancement of medical information, medical research, and health care delivery systems in our country.

So, Dr. Smith, thank you for coming, and while I will not be here to hear your testimony, I have read it, and it is excellent, and I think that this hearing will help to put us on the right track in making sure that these regulations, if they become final, strike the right balance between the important goal of individuals' medical

privacy and the advancement of medicine. So we appreciate your participation and all of those who are on the panels today.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Hutchinson.

I am pleased now to welcome our first witness this morning, who represents the U.S. General Accounting Office.

Ms. Leslie G. Aronovitz is director of health care, program administration and integrity issues at GAO in Chicago. She has spent the past 9 years at GAO as a director in the area of health, having also worked on income security issues. She is a certified public accountant and a graduate of the University of Georgia. She also received an M.B.A. from Boston University, concentrating on public management. A recipient of numerous professional awards, she was recognized with GAO's Distinguished Service Award in 1999. Congratulations.

Good morning. We are delighted to have you with us. Please proceed.

STATEMENT OF LESLIE G. ARONOVITZ, DIRECTOR, HEALTH CARE, PROGRAM ADMINISTRATION AND INTEGRITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE, CHICAGO, IL

Ms. ARONOVITZ. Thanks very much. I am delighted to be here.

Mr. Chairman and members of the committee, we are pleased to be here today as you discuss the new Federal regulation covering privacy of personal health information. The Congress required the creation of a health information privacy standard as part of the Health Insurance Portability and Accountability Act of 1996, as Senator Kennedy mentioned. It is related to several administrative simplification standards that HIPAA authorized to streamline health care paperwork.

As the committee requested, my remarks today will focus on highlights of the health privacy regulations published last December by the Department of Health and Human Services and will touch on the views we obtained from diverse affected parties.

As you know, the health privacy regulation was developed in a climate of dual concerns. Patients are troubled about the ability of providers and others to maintain confidentiality of their medical records in this electronic age of instantaneous transmission.

At the same time, payers, providers, researchers and others are worried about the ability to collect sufficient information to monitor health care quality, conduct clinical research, and pay claims appropriately, among a host of other critical uses of personal health information.

In text introducing the regulation, HHS stresses its attempt to balance these sometimes conflicting goals. Specifically, the regulation contains several "firsts" in privacy protection. For the first time, all Americans, regardless of the State they live or work in, can view and copy their medical records, request that errors be corrected, and get a history of authorized disclosures.

For the first time, it will be a Federal offense for doctors, hospitals, and health plans to disclose a patient's medical information to a bank, a life insurance company, or other nonhealth care user without first getting the patient's explicit authorization.

And for the first time, key players in the health care community, among them, doctors, hospitals, and health plans, will be required to establish a defined set of privacy-conscious business practices. They will also have to, through contracts, ensure that the individuals and firms they do business with implement certain privacy safeguards.

We discussed these and other features of the regulation with 17 national organizations representing patients, health care providers, accrediting bodies, State officials, employers, insurance companies, research and pharmaceutical groups. We also spoke with responsible HHS officials.

Incidentally, when these interviews were conducted 2 to 3 weeks ago, the noise level from the industry groups was much lower than the views that you will hear expressed here today. Most groups we interviewed said that HHS was responsive in addressing many of their concerns on the proposed regulation. However, given the newness, breadth, and complexity of the regulation, they also expressed uncertainty about what they needed to do to comply, and they wanted us to hold their comments as preliminary comments.

One controversial topic was this question of partial preemption. That is, under HIPAA authority, the Federal regulation does not preempt or override State laws with stronger privacy protections. The patient advocacy groups we spoke with favored the potential for State preemption because it prevents the Federal Government from withdrawing protections the States have already granted or may grant in the future.

In contrast, the insurer and employer advocates felt that the Federal Government should set a uniform national standard for protecting health privacy so that firms operating in more than one State will not have to content with figuring out which of the various State laws supersede the Federal regulation. Although these firms must already comply with an existing mix of State health privacy laws, they view the Federal requirements as an additional regulatory burden.

Another of the regulation's hot button issues pertains to the marketing and fund raising provisions. Under these provisions, doctors and hospitals are not allowed to give out any personal health information to a third party without the patient's expressed consent. But they can, without patient consent, mail commercial literature on behalf of the third party, as well as allow patients the option not to receive future appeals, identify themselves as the source of the marketing appeal, and State whether they are getting paid for this promotion.

The patient advocate groups we spoke with felt that these provisions could arguably be seen as a loophole in the Government's protection of personal health information and thought that giving patients the opportunity to opt out in advance of all marketing materials would better reflect the public's chief concern in this area.

Some of the groups' concerns were "how to" or implementation questions. For example, one group wanted to know how hospitals would obtain written consent from a patient at home prior to getting the necessary preadmission information for the patient's next-day surgery. Pharmacists questioned how to get consent from a

first-time patient whose prescription had been phoned in by the patient's physician and picked up by a family member.

Related to the implementation concerns were the comments by industry groups about the sheer cost associated with compliance, such as training employees, enhancing computer systems, tracking disclosures, and developing forms, notices, and contracts.

At this time, doctors, hospitals, health plans, and other covered entities face a complex set of requirements that are not well-understood. Some of the uncertainty reflects the recent issuance of the regulation. With time, everyone will have greater opportunity to examine its provisions and assess its implications.

For now, the affected parties have mixed feelings regarding the flexibility in the regulation to develop their own policies and procedures. The groups generally applaud this approach, but say that greater specificity would likely erase some of their compliance concerns.

Mr. Chairman and members of the committee, this concludes my prepared comments. I will be happy to answer any questions that you have.

[The prepared statement of Ms. Aronovitz follows:]

PREPARED STATEMENT OF LESLIE G. ARONOVITZ

Mr. Chairman and Members of the Committee: We are pleased to be here today as you discuss the new federal regulation covering the privacy of personal health information. Advances in information technology, along with an increasing number of parties with access to identifiable health information, have created new challenges to maintaining the privacy of an individual's medical records. Patients and providers alike have expressed concern that broad access to medical records by insurers, employers and others may result in inappropriate use of the information. Congress sought to protect the privacy of individuals' medical information as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA included a timetable for developing comprehensive privacy standards that would establish rights for patients with respect to their medical records and define the conditions for using and disclosing identifiable health information. In December 2000, the Department of Health and Human Services (HHS) released the final regulation on privacy standards. The regulation requires that most affected entities comply by February 26, 2003.

In April 2000, we testified on HHS' proposed privacy regulation. At that time, we noted that the comments made by the affected parties reflected two overriding themes. The first was a widespread acknowledgment of the importance of protecting the privacy of medical records. The second reflected the conflicts that arise in attempts to balance protecting patients' privacy and permitting the flow of health information for necessary uses. Last month, the Committee requested that we obtain the perspectives of affected parties regarding the regulation. My remarks today will focus on (1) the rights of patients and the responsibilities of the entities that use personal health information, as set forth in the federal privacy regulation and (2) the concerns of key stakeholders regarding the regulation's major provisions. In gathering this information, we contacted 17 national organizations representing patients, health care providers, accrediting bodies, state officials, employers, insurance companies, and research and pharmaceutical groups. (A list of these organizations is in the appendix.) We also reviewed the regulation and spoke with HHS officials responsible for implementing it. We performed our work in January 2001 in accordance with generally accepted government auditing standards.

In brief, the regulation acts as a federal floor (to be superseded by state privacy regulations that are more stringent) in establishing standards affecting the use and disclosure of personal health information by providers, health plans, employers, researchers, and government agencies. Patients will have increased knowledge about, and potential control over, what information is shared, with whom, and for what purposes. At the same time, entities that receive personal health information will be responsible for ensuring that the information is effectively protected.

Most groups we interviewed acknowledged that HHS was responsive in addressing many of their comments on the draft regulation. However, given the newness,

breadth, and complexity of the regulation, they also expressed uncertainty about all that organizations may need to do to comply. Many raised questions about the requirements for entities to obtain patient consent or authorization prior to disclosing or using personal health information. Other concerns focused on how regulated entities will apply the privacy provisions to their business associates. Most groups focused on the HIPAA provision that more stringent state privacy requirements preempt the federal regulation. Some groups favored this flexibility, whereas others asserted that the lack of a single set of privacy standards will add regulatory burden. Finally, many organizations raised questions about the feasibility and cost of implementing the regulation in the time allotted.

BACKGROUND

The federal privacy regulation is the second of nine administrative simplification standards to be issued under HIPAA that HHS has released in final form. In addition to information privacy, the standards are to address transaction codes and medical data code sets; consistent identifiers for patients, providers, health plans, and employers; claims attachments that support a request for payment; data security; and enforcement. Taken together, the nine standards are intended to streamline the flow of information integral to the operation of the health care system while protecting confidential health information from inappropriate access, disclosure, and use.

HIPAA required the Secretary of HHS to submit recommendations to the Congress on privacy standards, addressing (1) the rights of the individual who is the subject of the information; (2) procedures for exercising such rights; and (3) authorized and required uses and disclosures of such information. HIPAA further directed that if legislation governing these privacy standards was not enacted within 3 years of the enactment of HIPAA—by August 21, 1999—the Secretary should issue regulations on the matter. HHS submitted recommendations to Congress on September 11, 1997, and when legislation was not enacted by the deadline, issued a draft regulation on November 3, 1999. After receiving over 52,000 comments on the proposed regulation, HHS issued a final regulation on December 28, 2000.

Two key provisions in HIPAA defined the framework within which HHS developed the privacy regulation.

HIPAA specifically applies the administrative simplification standards to health plans, health care clearing houses (entities that facilitate the flow of information between providers and payers), and health care providers that maintain and transmit health information electronically. HHS lacks the authority under HIPAA to directly regulate the actions of other entities that have access to personal health information, such as pharmacy benefit management companies acting on behalf of managed care networks.

HIPAA does not allow HHS to preempt state privacy laws that are more protective of health information privacy. Also, state laws concerning public health surveillance (such as monitoring the spread of infectious diseases) may not be preempted.

HIPAA does not impose limits on the type of health care information to which federal privacy protection would apply. At the time the proposed regulation was issued, HHS sought to protect only health data that had been stored or transmitted electronically, but it asserted its legal authority to cover all personal health care data if it chose to do so. HHS adopted this position in the final regulation and extended privacy protection to personal health information in whatever forms it is stored or exchanged—electronic, written, or oral.

PRIVACY REGULATION ESTABLISHES NEW RIGHTS AND RESPONSIBILITIES

The new regulation establishes a minimum level of privacy protection for individually identifiable health information that is applicable nationwide. When it takes full effect, patients will enjoy new privacy rights, and providers, plans, researchers, and others will have new responsibilities. Most groups have until February 26, 2003 to come into compliance with the new regulation, while small health plans were given an additional year.

Patients' Rights

The regulation protecting personal health information provides patients with a common set of rights regarding access to and use of their medical records. For the first time, these rights will apply to all Americans, regardless of the state in which they live or work. Specifically, the regulation provides patients the following:

Access to their medical records. Patients will be able to view and copy their information, request that their records be amended, and obtain a history of authorized disclosures.

Restrictions on disclosure. Patients may request that restrictions be placed on the disclosure of their health information. (Providers may choose not to accept such requests.) Psychotherapy notes may not be used by, or disclosed to, others without explicit authorization.

Education. Patients will receive a written notice of their providers' and payers' privacy procedures, including an explanation of patients' rights and anticipated uses and disclosures of their health information.

Remedies. Patients will be able to file a complaint with the HHS Office for Civil Rights (OCR) that a user of their personal health information has not complied with the privacy requirements. Violators will be subject to civil and criminal penalties established under HIPAA.

Responsibilities of Providers, Health Plans, and Clearing houses

Providers, health plans, and clearing houses—referred to as covered entities—must meet new requirements and follow various procedures, as follows:

Develop policies and procedures for protecting patient privacy. Among other requirements, a covered entity must designate a privacy official, train its employees on the entity's privacy policies, and develop procedures to receive and address complaints.

Obtain patients' written consent or authorization. Providers directly treating patients must obtain written consent to use or disclose protected health information to carry out routine health care functions. Routine uses include nonemergency treatment, payment, and an entity's own health care operations. In addition, providers, health plans, and clearing houses must obtain separate written authorization from the patient to use or disclose information for nonroutine purposes, such as releasing information to lending institutions or life insurers.

Limit disclosed information to the minimum necessary. Covered entities must limit their employees' access to identifiable health information to the minimum needed to do their jobs. When sharing personal health information with other entities, they must make reasonable efforts to limit the information disclosed to the minimum necessary to accomplish the purpose of the data request (such as claims payment). However, they may share the full medical record when the disclosure is for treatment purposes.

Ensure that "downstream users" protect the privacy of health information. Covered entities must enter into a contract with any business associates with which they share personal health information for purposes other than consultation, referral, or treatment. Contracts between covered entities and their business associates must establish conditions and safeguards for uses and disclosures of identifiable health information. Covered entities must take action if they know of practices by their business associates that violate the agreement.

Adhere to specific procedures in using information for fund raising or marketing. Covered entities may use protected patient information to develop mailing lists for fund raising appeals, but they must allow patients to choose not to receive future appeals. Similarly, while patient authorization is required to transmit personal health information to a third party for marketing purposes, a covered entity (or its business associate) can itself use such data for marketing on behalf of a third party without authorization. In such cases, the entity must identify itself as the source of the marketing appeal, state whether it is being paid to do so, and give recipients the opportunity to opt out of receiving additional marketing communications.

Protect unauthorized release of medical records to employers. Group health plans must make arrangements to ensure that personal health information disclosed to the sponsors, including employers, will not be used for employment-related purposes, such as personnel decisions, without explicit authorization from the individual. Furthermore, where staff administering the group health plan work in the same office as staff making hiring and promotion decisions, access to personal health information must be limited to those employees who perform health plan administrative functions.

Responsibilities of Researchers

The regulation sets out special requirements for use of personal health information that apply to both federal and privately funded research:

Researchers may use and disclose health information without authorization if it does not identify an individual. Information is presumed to be de-identified by removing or concealing all individually identifiable data, including name, addresses, phone numbers, Social Security numbers, health plan beneficiary numbers, dates indicative of age, and other unique identifiers specified in the regulation.

Researchers who seek personal health information from covered entities will have two options. They can either obtain patient authorization or obtain a waiver from

such authorization by having their research protocol reviewed and approved by an independent body—an institutional review board (IRB) or privacy board. In its review, the independent body must determine that the use of personal health information will not adversely affect the rights or welfare of the individuals involved, and that the benefit of the research is expected to outweigh the risks to the individuals' privacy.

Responsibilities and Rights of Federal Agencies and State Governments

HHS and others within the federal government will have a number of specific responsibilities to perform under the regulations. Although it no longer falls to the states to regulate the privacy of health information, states will still be able to enact more stringent laws.

Federal and state public officials may obtain, without patient authorization, personal health information for public health surveillance; abuse, neglect, or domestic violence investigations; health care fraud investigations; and other oversight and law enforcement activities.

HHS' OCR has broad authority to administer the regulation and provide guidance on its implementation. It will decide when to investigate complaints that a covered entity is not complying and perform other enforcement functions directly related to the regulations. HIPAA gives HHS authority to impose civil monetary penalties (\$100 per violation up to \$25,000 per year) against covered entities for disclosures made in error. It may also make referrals for criminal penalties (for amounts of up to \$250,000 and imprisonment for up to 10 years) against covered entities that knowingly and improperly disclose identifiable health information.

CONCERNS BY STAKEHOLDERS REFLECT COMPLEXITY OF THE REGULATION

Among the stakeholder groups we interviewed, there was consensus that HHS had effectively taken into account many of the views expressed during the comment period. Most organizations also agreed that the final regulation improved many provisions published in the proposed regulation. At the same time, many groups voiced concerns about the merit, clarity, and practicality of certain requirements.

Overall, considerable uncertainty remains regarding the actions needed to comply with the new privacy requirements. Although the regulation, by definition, is prescriptive, it includes substantial flexibility. For example, in announcing the release of the regulation, HHS noted that "the regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity." Among the stakeholder groups we interviewed, the topics of concern centered on conditions for consent, authorization, and disclosures; rules pertaining to the business associates of covered entities; limited preemption of state laws; the costs of implementation; and HHS' capacity to provide technical assistance.

Consent and Disclosure Provisions Attracted a Range of Concerns

Several of the organizations we contacted considered the regulation's consent, authorization, or disclosure provisions a step forward in the protection of personal health information. However, several groups questioned the merits of some of the provisions. For example, representatives of patient advocacy groups—the National Partnership for Women and Families, the Health Privacy Project, and the American Civil Liberties Union—were concerned that the regulation permits physicians, hospitals, and other covered entities to market commercial products and services to patients without their authorization. One representative noted that commercial uses of patient information without authorization was an issue that provided the impetus for federal action to protect health privacy in the first place. Another representative commented that public confidence in the protection of their medical information could be eroded as a result of the marketing provisions. One representative also concluded that allowing patients the opportunity to opt out in advance of all marketing contacts would better reflect the public's chief concern in this area. HHS officials told us that this option exists under the provision granting patients the right to request restrictions on certain disclosures but that providers are not required to accept such patient requests.

Several organizations questioned whether the scope of the consent provision was sufficient. For example, American Medical Association (AMA) representatives supported the requirement that providers obtain patient consent to disclose personal health information for all routine uses, but questioned why the requirement did not apply to health plans. Plans use identifiable patient information for quality assurance, quality improvement projects, utilization management, and a variety of other purposes. The association underscored its position that consent should be obtained before personal health information is used for any purpose and that the exclusion

of health plans was a significant gap in the protection of this information. AMA suggested that health plans could obtain consent as part of their enrollment processes.

The American Association of Health Plans (AAHP) also expressed concerns about the scope of consent, but from a different perspective. AAHP officials believe that the regulation may limit the ability of the plans to obtain the patient data necessary to conduct health care operations if providers' patient consent agreements are drawn too narrowly to allow such data sharing. They suggested two ways to address this potential problem. First, if the health plans and network providers considered themselves an "organized health care arrangement," access to the information plans needed could be covered in the consent providers obtained from their patients. Second, plans could include language in their contracts with physicians that would ensure access to patients' medical record information.

Several organizations also had questions about how the consent requirement might be applied. For example, the American Pharmaceutical Association (APhA) raised concerns about how pharmacies could obtain written consent prior to treatment—that is, filling a prescription for the first time. The American Health Information Management Association (AHIMA) similarly noted the timing issue for hospitals with respect to getting background medical information from a patient prior to admission. HHS officials told us that they believe the regulation contains sufficient flexibility for providers to develop procedures necessary to address these and similar situations.

Research organizations focused on the feasibility of requirements for researchers to obtain identifiable health information. The regulation requires them to obtain patient authorization unless an independent panel reviewing the research waives the authorization requirement. Although this approach is modeled after long-standing procedures that have applied to federally funded or regulated research, the regulation adds several privacy-specific criteria that an institutional review board or privacy board must consider. The Association of American Medical Colleges and the Academy for Health Services Research and Health Policy expressed specific concerns over the subjectivity involved in applying some of the additional criteria. As an example, they highlighted the requirement that an independent panel determine whether the privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the value of the research involved.

Relationships Uncertain Regarding Covered Entities and Their Business Associates

Several groups were concerned about the requirement for covered entities to establish a contractual arrangement with their business associates—accountants, attorneys, auditors, data processing firms, among others—that includes assurances for safeguarding the confidentiality of protected information. This arrangement was HHS' approach to ensure that the regulation's protections would be extended to information shared with others in the health care system. Some provider groups we spoke with were confused about the circumstances under which their member organizations would be considered covered entities or business associates.

Some groups, including the Health Insurance Association of America (HIAA) and the Blue Cross and Blue Shield Association (BCBSA), questioned the need for two covered entities sharing information to enter into a business associate contract. The regulation addresses one aspect of this concern. It exempts a provider from having to enter into a business associate contract when the only patient information to be shared is for treatment purposes. This exemption reflects the reasoning that neither entity fits the definition of business associate when they are performing services on behalf of the patient and not for one another. An example of such an exemption might include physicians writing prescriptions to be filled by pharmacists.

Some groups also commented on the compliance challenges related to the business associate arrangement. For example, the representatives of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) noted that it would need to enter into contracts for each of the 18,000 facilities (including hospitals, nursing homes, home health agencies, and behavioral health providers) that it surveys for accreditation. However, JCAHO officials hope to standardize agreements to some extent and are working on model language for several different provider types. They explained that, because assessing quality of care varies by setting, JCAHO would need more than one model contract.

Views Divided on Partial Preemption of State Laws

Most of the groups we interviewed cited as a key issue the HIPAA requirement that the privacy standards preempt some but not all state laws. Although every state has passed legislation to protect medical privacy, most of these laws regulate particular entities on specific medical conditions, such as prohibiting the disclosure of AIDS test results. However, a few states require more comprehensive protection

of patient records. The patient advocacy groups we spoke with believe that partial preemption is critically important to prevent the federal rule from weakening existing privacy protections. According to the Health Privacy Project, the federal regulation will substantially enhance the confidentiality of personal health information in most states, while enabling states to enact more far-reaching privacy protection in the future.

Despite the limited scope of most state legislation at present, other groups representing insurers and employers consider partial preemption to be operationally cumbersome and argue that the federal government should set a single, uniform standard. Organizations that operate in more than one state, such as large employers and health plans, contend that determining what mix of federal and state requirements applies to their operations in different geographic locations will be costly and complex. Although they currently have to comply with the existing mix of state medical privacy laws, they view the new federal provisions as an additional layer of regulation. A representative of AHIMA remarked that, in addition to state laws, organizations will have to continue to take account of related confidentiality provisions in other federal laws (for example, those pertaining to substance abuse programs) as they develop policies and procedures for notices and other administrative requirements.

The final regulation withdrew a provision in the proposed regulation that would have required HHS to respond to requests for advisory opinions regarding state preemption issues. HHS officials concluded that the volume of requests for such opinions was likely to be so great as to overwhelm the Department's capacity to provide technical assistance in other areas. However, they did not consider it unduly burdensome or unreasonable for entities covered by the regulation to perform this analysis regarding their particular situation, reasoning that any new federal regulation requires those affected by it to examine the interaction of the new regulation with existing state laws and federal requirements.

Stakeholders Believe Compliance Challenges May Be Costly

Several groups in our review expressed concern about the potential costs of compliance with the regulation and took issue with HHS' impact analysis. In that analysis, the Department estimated the covered entities' cost to comply with the regulation to be \$17.6 billion over the first 10 years of implementation. Previously, HHS estimated that implementation of the other administrative simplification standards would save \$29.9 billion over 10 years, more than offsetting the expenditures associated with the privacy regulation. HHS therefore contends that the regulation complies with the HIPAA requirement that the administrative simplification standards reduce health care system costs.

HHS expects compliance with two provisions--restricting disclosures to the minimum information necessary and establishing a privacy official--to be the most expensive components of the privacy regulation, in both the short and the long term. Table 1 shows HHS' estimates of the costs to covered entities of complying with the privacy regulation.

Table 1: HHS' Cost Estimates for Implementing Privacy Regulation Provisions (Millions of Dollars)

Requirements	First-year costs (2003)	10-year costs (2003-12)
Disclose only minimum necessary information	\$926.2	\$5,756.7
Designate a privacy official	723.2	5,905.8
Develop policies and procedures	597.7	597.7
Establish business associate contracts	299.7	800.3
Train employees in privacy policies	287.1	737.2
Track authorized disclosures	261.5	1,125.1
Obtain consent to use patient information	166.1	227.5
De-identify protected health information	124.2	1,177.4
Modify health information for employer use (applies to group health plans)	52.4	52.4
Prepare and distribute notice of privacy practices	50.8	391.0
Obtain IRB or privacy board approval for research	40.2	584.8
Implement a process for individuals to file complaints	6.6	103.2
Amend patient medical records on request	5.0	78.8
Process patient requests to inspect and copy their medical records	1.3	16.8
Total	3,542.0	17,554.7

Source: *Federal Register*, Dec. 28, 2000, page 82761.

We did not independently assess the potential cost of implementing the privacy regulation, nor had the groups we interviewed. However, on the basis of issues raised about the regulation, several groups anticipate that the costs associated with compliance will exceed HHS' estimates. For example, BCBSA representatives contended that its training costs are likely to be substantial, noting that its member plans encompass employees in a wide range of positions who will require specialized training courses. AHA cited concerns about potentially significant new costs associated with developing new contracts under the business associate provision. Other provider groups anticipated spending additional time with patients to explain the new requirements and obtain consent, noting that these activities will compete with time for direct patient care. Several groups, including AHA, AAMC, and AHIMA, expressed concerns about being able to implement the regulation within the 2-year time frame.

Despite their concerns, several groups discussed possible actions that could help mitigate the anticipated administrative burden. For example, AHA plans to develop model forms for patient consent forms, notices explaining privacy practices, business associate contracts, and compliance plans. Representatives of APHA similarly intend to give their members model forms, policies, and procedures for implementing the regulation. AMA expects to provide guidance to physicians and help with forms and notices on a national level, and noted that the state medical associations are likely to be involved in the ongoing analysis of each state's laws that will be required.

HHS' Capacity to Assist With Implementation Questioned

Representatives of some organizations we contacted commented that they were unsure how the Department's OCR will assist entities with the regulation's implementation. They anticipate that the office, with its relatively small staff, will experience difficulty handling the large volume of questions related to such a complex regulation. OCR officials informed us that the office will require additional resources

to carry out its responsibilities and that it is developing a strategic plan that will specify both its short- and its long-term efforts related to the regulation.

To carry out its implementation responsibilities, HHS requested and received an additional \$3.3 million in supplemental funding above its fiscal year 2001 budget of approximately \$25 million. According to OCR, this amount is being used to increase its staff of 237 to support two key functions: educating the public and those entities covered by the rule about the requirements and responding to related questions. OCR officials told us that its efforts to date include presentations to about 20 organizations whose members are affected by the regulation, a hotline for questions, and plans for public forums.

OCR officials said the Office had received about 400 questions since the regulation was issued. Most of these inquiries were general questions relating to how copies of the regulation can be obtained, when it goes into effect, and whether it covers a particular entity. Other questions addressed topics such as the language and format to use for consent forms, how to identify organized health care arrangements, whether the regulation applies to deceased patients, and how a patient's identity should be protected in a physician's waiting room. According to OCR officials, technical questions that cannot be answered by OCR staff are referred to appropriate experts within HHS.

CONCLUSION

The final privacy regulation represents an important advancement in the protection of individuals' health information. It offers all Americans the opportunity to know and, to some extent, control how physicians, hospitals, and health plans use their personal information. At the same time, these entities will face a complex set of privacy requirements that are not well understood at this time. Some of the uncertainty expressed by stakeholder groups reflects the recent issuance of the regulation. With time, everyone will have greater opportunity to examine its provisions in detail and assess their implications for the ongoing operations of all those affected. In addition, on a more fundamental level, the uncertainty stems from HHS' approach of allowing entities flexibility in complying with its requirements. Although organizations generally applaud this approach, they acknowledge that greater specificity would likely allay some of their compliance concerns.

The CHAIRMAN. Thank you very much.

I am interested in hearing about what HHS will be doing to help covered entities comply with the new requirements. Is there a process in the rule that covered entities can employ to determine which State laws are and are not preempted?

Ms. ARONOVITZ. The responsibility for educating all parties involved with this privacy act and also in enforcing the act is put in HHS' Office for Civil Rights. That office is in the process right now of trying to get organized and figure out what type of privacy education enforcement strategy it will employ.

At one point and during its comment period, HHS heard many requests to be able to look at State laws and issue State-by-State guidance or in some way advisory opinions on what State laws would preempt the Federal regulation. HHS has now backed off on their willingness to do that in that they feel that their guidance would only be advisory, and in fact, they do not have the resources to be able to provide those kinds of assurances. Instead, they feel that State medical societies and other groups will work with the covered entities and others to try to develop that kind of information. They do feel that it is the covered entity's responsibility to make those determinations on its own.

In terms of what types of activities the Office for Civil Rights will be doing, they did ask for a \$3 million increase in their budget to staff the Office for Civil Rights to provide privacy-type activities. They do feel that they want to spend the first 2 years during the implementation time educating different parties as to what the rule requires.

The CHAIRMAN. I think we will want to watch that closely to make sure the information is available. Thank you.

What limitations if any does the rule impose on marketing and fund raising activities, and what are the differences between how the rule treats marketing versus fund raising activities?

Ms. ARONOVITZ. Marketing and fund raising clearly is a hot button in this regulation. The people who talked about it felt very fervently that there is a visceral concern on the part of people who worry about health privacy that people will get marketing materials, and they will feel as though someone is abusing their information for someone else's profit.

On the other hand, one of the reasons why HHS told us they felt that the marketing and fund raising provisions should be in the regulation is that there were a lot of activities that could be in a patient's best interest in terms of health promotion and other types of new advances in technology that would in fact educate patients on how to best access the health care system.

Although a lot of those health promotion activities are really part of a covered entity's health care operations, there was a lot of concern that the definition of health care operations might fall or might be construed as being marketing, so they gave that permission.

The difference is that as far as marketing goes, a covered entity could market on behalf of a third party but would not be able to give the third party the information that they have. They also have to inform the patient whom they are marketing on behalf of and also that they are getting paid, if they are, by a third party. They also have to give that patient the opportunity to opt out of future mailings.

In marketing, it can be diagnosis-oriented. In other words, a marketing as covered entity could identify all the cancer patients who came to that hospital and say that we have some new advances in the treatment that you might be interested in.

For fund raising purposes, institutions cannot market by virtue of specific diagnoses. They have to market for the whole population.

The CHAIRMAN. What legal authority does HHS have to extend privacy protections to paper and oral information, rather than just limiting the protections to the information maintained or shared in the electronic format, as was the scope of the proposed rule?

Ms. ARONOVITZ. The proposed rule really only covered electronic information, and they got a lot of comments that said that to a great extent, it would be simpler if paper records and oral communication were not discussed as much in the comments, but that at least for paper records, it would be simpler if that could be covered. There are some concerns now about oral communications and how workable that would be in certain situations, and I am sure that you will hear about that. But on the whole, the groups we spoke with feel comfortable that covering paper records is an improvement from the proposed regulation. The biggest concern now is really how to make it workable.

HHS felt that it had the authority in HIPAA to extend the rule to paper and oral communications, and we agree that the process that they went through to decide that is reasonable, and therefore,

we would defer to their judgment and agree that that would be included.

The CHAIRMAN. Senator Kennedy.

Senator KENNEDY. Thank you very much, Mr. Chairman.

I thank you for a very complete report, Ms. Aronovitz. Picking up on what the chairman has pointed out, I was particularly pleased to hear you say that the GAO agrees with HHS on the legality of their extension of privacy protection to all medical records and offices that use electronic transactions. I think this is an extremely important decision on the part of HHS and I believe it will best serve both the American people and the health care industry.

Other witnesses today are going to express some concerns about the vague nature of some of the requirements in the regulation. Given your professional experience at GAO and the 2-year implementation time frame of this regulation, is it your belief that this can provide periodic and specific guidance during the next 2 years that will clarify the privacy requirements?

Ms. ARONOVITZ. Clearly, HHS has an uphill battle. They really have to gear up and get organized. They have to identify people in their organization who have the ability and the expertise to be able to work out what will be considered to be many, many interpretations and questions that they are going to be receiving.

We have heard all kinds of scenarios, and we think a lot of them have to do with interpretive concerns and some implementation concerns.

When we talk to HHS about how they want to deal with these concerns, they believe that over time, covered entities will work through some of the concerns they have and come up with workable solutions. Some of the groups we talked to absolutely feel that this is such a burden that it would be impossible for them to work through everything they need to in the 2-year implementation time frame that they have. Many that we spoke with would like to have that time extended.

We believe that this is definitely going to be a challenge, and depending on individual covered entity situations, they will need to work through some of these rules.

Senator KENNEDY. I would just point out that 2 years is a long time, and there are important protections out there, so I know there will be pressure for additional time. I would hope that the interested groups would understand the importance that many of us put on that 2-year time frame.

Let me move to the research provisions of this regulation. Some in the research community are concerned about the requirement that the IRBs and the privacy boards must weigh privacy risks with value of the knowledge to be gained by the research. But, they currently conduct a similar weighing of risk in terms of the benefit to the research subject. Isn't it appropriate to weigh the privacy considerations when sensitive medical information is involved?

Ms. ARONOVITZ. Absolutely. It is just that it is something that IRBs do not typically do on a patient-specific basis, and in this rule, the IRB would have to consider the benefit to the research versus the privacy protections or the privacy risks for the population and each individual. That is a new criterion.

Senator KENNEDY. In any event, the IRB has to consider the medical effects of any procedure on the patients themselves, so, how much of an additional burden do you really think this requirement to look at privacy will place on them?

Ms. ARONOVITZ. The biggest issue in terms of burden really has to do with the subjectivity that these groups feel the IRB will be up against. They feel that it will be very difficult in some cases to make those judgments and get consensus that those judgments are correct.

Senator KENNEDY. Quickly, could you give an indication of what the costs of this regulation are, and also an indication of what you think the savings would be because of the other incentives in HIPAA for using electronic media more effectively? I have seen that the costs are only a fraction of one percent in terms of health care costs over the future. I know you have a good deal of information on it, but for the benefit of the hearing, could you give that to us quickly?

Ms. ARONOVITZ. Yes. We did not do an independent cost-benefit analysis, but HHS did do an analysis that said that the complete set of rules in HIPAA, not just the privacy rules, ultimately will save almost \$30 billion. The privacy rule will cost about \$17 billion, and therefore—I might not have my numbers right—there are quite a lot of costs associated with the privacy rule, but ultimately, the overall HIPAA regulations will still have a net savings of about \$12 billion.

Senator KENNEDY. I think that for all Americans, privacy is what they are interested in. But, we are also doing this in a very efficient way that actually can save resources over a period of time as well.

Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Kennedy.

Senator Roberts.

Senator ROBERTS. Thank you, Mr. Chairman.

I am new to the committee, and first, I want to thank you very much for your testimony. GAO has been very helpful in the past on these issues.

Mr. Chairman, I was chairman of the Rural Health Care Coalition in the House, and I can remember many battles we have had where we have tried to guarantee some things and tried to improve the quality of health care only to find out in the rural health care delivery system that we were really posing great hardships for the 100 hospitals in Kansas with 50 beds or less.

So I have been reading the testimony, and staff has been bringing me up-to-date, and I sort of sighed, and I said, "By golly, here we go again."

I guess I should emphasize that we all support the goal behind these regulations. I understand that. The privacy of the records is critically important to all of us. We have some real horror stories that have received a lot of publicity, and the pain and hardship that people go through—we have to do a better job. I question this.

I tried to sit down and read the regulations, just as a hospital administrator, the belabored hospital administrators, and here they are again. We used to do this with the coalition efforts—I think that probably Craig Thomas does it over here—and I defy anybody

to read through that. But the hospital administrators have to do that, and their board members have to do that, to find out how on earth we are going to comply.

I know that the bill was passed 2 years ago. My colleague in the Senate, Senator Kassebaum, and the distinguished Senator from Massachusetts worked very hard, and we were unable to come up with regulations here in the Congress—we are pretty good at that—so we gave it to HHS, and now we have these regulations. And I can tell you the Kansas Hospital Association with whom I have been working for 25 or 30 years is terribly concerned.

I am not sure that all this paperwork is going to do the job that it is intended to do, but we have no alternative but to see if we cannot make it work.

I understand there is a grace period of 1 year for small health plans whose annual receipts are \$5 million or less before they have to be in compliance with the new regs. As I have indicated, we have 100 hospitals with 50 beds or less, and we are just darned glad to have them. We have nurse shortages, we have doctor shortages, we have hospitals where you have to travel 50, 60, 150 miles just to get the care. And we already have the “bad news bear” person who is designated in regard to trying to comply with all the regulations—I will not get into that—in terms of Medicare reimbursement and all of that.

They are struggling to keep the doors open. Almost every hospital, every community, has had to pass a bond issue on top of what would normally be a positive cost-share kind of payment from the Federal Government with all the obligations they have had. I am terribly worried about how we are able to obtain the kind of professional person who will be able to do the job or retrain somebody that we simply do not have.

Is there any similar grace period for the small health care provider that you are aware of?

Ms. ARONOVITZ. Actually, the grace period that you speak of is an additional year over the 2 years that providers and health plans and clearing houses have to completely implement the rule, so that small health plans with receipts under \$5 million would have 3 years, or would actually have until February 26, 2004 to implement the regulation. It does not apply right now to small health providers.

Senator ROBERTS. I can complain about these regs all the time and give my speech about how we are regulating the rural health care delivery system out of business. That is not going to do any good. We have got to come up with these people.

In your research, do you anticipate that training a new person already there—and I am not sure how we do that—will be adequate in terms of meeting these criteria, or are we going to have to have some kind of a crash training program in Kansas and other States to bring people on? I guess I am asking the question in terms of an on-site person; I do not know who is going to be that utility infielder.

Ms. ARONOVITZ. I think that as you will hear with this regulation, there is no definitive answer to any of these questions. I think it is very situational, depending on the size and situation and types of activities that are carried on. It might not be that difficult to

train somebody who is already experienced in dealing with consent forms and dealing with the types of activities that very often occur right now in terms of protecting privacy.

On the other hand, one of the major cost areas that groups have talked to us about—mostly the large covered entities—will be in additional training costs.

Senator ROBERTS. I only have a minute or maybe 30 seconds left. I looked at the chart provided by the Kansas Hospital Association on the business associates contracting requirement. The hospital is not only responsible for the hospital but for anywhere between 50 and 750 business partner contracts per hospital. I would love to have 750 business partners in rural America with a hospital, but how on earth is that person going to be responsible for all these folks?

Ms. ARONOVITZ. They do have to write contracts, and the hope is that a lot of those contracts will be standard contracts based on routine activities that are performed by physicians.

Senator ROBERTS. The funeral homes and the clergy and the housekeeping and the plant security guards and the maintenance building and the laboratory testing and the outside imagining—I can go on and on—I am a little stunned by all of this. And I apologize for coming to the issue late, but I do not know how we are going to comply with this.

Ms. ARONOVITZ. I in no way want to be an apologist for this reg, but I do know that there are certain provisions for organized health care arrangements or employees who are part of that hospital system, so there might be ways to narrow down the number of business associates that that hospital actually has, although there is no doubt that this is definitely going to be an area that is going to create at least an initial burden in terms of rewriting those contracts.

Senator ROBERTS. We may have a job for you out there in Kansas if you would like to relocate.

The CHAIRMAN. Senator Dodd?

Senator DODD. Thank you very much, Mr. Chairman.

I will ask unanimous consent that my opening statement be included in the record regarding the subject matter.

The CHAIRMAN. Without objection.

[The prepared statement of Senator Dodd follows:]

PREPARED STATEMENT OF SENATOR DODD

Mr. Chairman, thank you for convening this oversight hearing on the medical privacy regulation recently issued by the Department of Health and Human Services. I also want to thank the General Accounting Office for its report to the committee on the new rights and responsibilities created by the regulation and the major concerns of stakeholders.

We live in an era in which information can travel around the world in the blink of an eye—an advance in technology that has already dramatically improved the delivery of health care. But, while many of our constituents embrace the benefits of the information age, they remain deeply concerned about what they perceive to be a loss of control over their sensitive, personal information—whether financial, medical, or genetic.

There is a growing fear that technology is being used not to improve our lives, but to make it easier for others to rifle through our medicine cabinets and peer into our checkbooks.

In the simplest terms, consumers want the "right to know" and the right to say no" to the sharing of their personal information.

I think it's fair to say that prior to this new regulation, they didn't have those rights when it came to their medical records. By and large, with the exception of a few state laws, all consumers had standing between them and the misuse of their information were good intentions, professional ethics and internal company policies.

With this regulation, for the first time, consumers will have the right to see their own records. For the first time, health care providers will have to get a patient's consent before sharing medical information. For the first time, firewalls will be placed in the workplace between the people who run the employer's health insurance program and those who make hiring and firing decisions. These new rights, and the many others provided by the regulation, are truly a historic step forward.

Having worked for more than two years with Senator Jeffords to craft what became the only bipartisan Senate medical privacy legislation, I understand just how tough a job it is to get it right when it comes to crafting privacy protections. Given the complexity of our health care system, figuring out how to give consumers control over their medical records without disrupting the flow of information needed to make the health care system work is a formidable task. So, I want to commend the Clinton administration for its success in creating a strong base of federal protections for medical records.

It is clear, however, that there is still more to be done when it comes to protecting the privacy of medical records. Secretary Shalala was limited by law in the scope of the protections she could give. For example, she could not directly regulate the use of medical information by employers and drug companies. And, she could not offer individuals whose rights are violated the opportunity to seek legal redress. These are protections only Congress can give and it is my hope that we will act quickly to plug these holes.

And, beyond the work remaining on medical records, it is my hope that this Congress will be known as one that took bold, purposeful steps to restore personal privacy in all its forms. As a new co-chair of the bipartisan, bicameral Congressional Privacy Caucus—along with Senator Shelby, and Congressmen Markey and Barton—I would like to see us work across committee and party lines to address the pervasive concerns of the public about the full range of threats to privacy. In my view, if we fail to deal with this issue comprehensively, we will see a backlash from the public of a sufficient magnitude to negate the promise that information technology holds for improving the lives of all Americans.

Thank you again Mr. Chairman for holding this hearing. I look forward to the testimony of our witnesses.

Senator DODD. I would note that you and I worked for more than 2 years to develop the first real bipartisan piece of legislation dealing with medical records, and my hope is that we will be able to continue that work here, and obviously, the step which has been taken by the previous administration to promote some regulations

in this area I think is a positive step forward, so I want to thank the General Accounting Office once again for their fine work in this area.

This is an issue that is transcendent in many ways. I have told this anecdote on numerous occasions, but about 8 years ago when I first became interested in this subject matter in preparation for a campaign, I included language gaging people's interest in privacy—I did not get specific about medical records or financial records, genetic information, or Internet access and so forth—and it exceeded every other issue in my State by almost 20 points when it came back. And it was not a complicated question; it was just the issue of privacy. It just stunned me how positively and forcefully my constituency stated to their concerns about whether or not information that they had long felt was private or should be private was just too accessible to too many people. No issue is more sensitive for people than their private medical information and what may happen with it.

So this is a very important hearing, and your study is an extremely important study, but I am somewhat concerned—and I think you share this view—that not unlike the portability issue with insurance policies, when we adopted that, there was a raft of people who assumed they could just pick up and move wherever they wanted to and carry their insurance policies around with them. They discovered that the law was far more complex than they thought it was much more difficult than they had anticipated.

In a sense, while there are regulations that are very positive, Donna Shalala was somewhat limited in terms of what she could actually do and how far HIPAA could reach in protecting people's privacy with regard to medical records, and that is the first question I would like to touch on with you, if I could.

Because of the restrictions as I understand them—and I do not claim to be a great expert on HIPAA, but I understand there are restrictions, which you have mentioned—in fact, many of the major users of medical information, like pharmaceutical companies, life insurers, Internet websites and the like, would not be directly covered by these new regulations. Is that correct?

Ms. ARONOVITZ. Absolutely—it is clear that a life insurer would not be covered, because they do not get involved in direct health care treatment. But if a website is actually treating someone, they could possibly be construed as being a covered entity. It is very specific to the nature of their operations.

Senator DODD. That is my point. It does try to reach some of those users, but the protections are rather incomplete.

Ms. ARONOVITZ. Yes.

Senator DODD. For instance, if you ask people who they would be most concerned about having their medical information, I presume one of the top answers would be the employer, in terms of potential job discrimination, firing, insurance coverage, and so on. Yet employers who collect direct health information from their employees—from a worksite health clinic, for example, which is not an uncommon practice at all—are not subject to the regulation, as I understand it. Is that correct?

Ms. ARONOVITZ. That is right. An employer who is sponsoring or administering a health plan would have information pursuant to

their activities in sponsoring that health plan. But in employment decisions, promotion decisions, or any other type of activity that is nonhealth-related, the employer would not have access to that protected information.

Senator DODD. What about a worksite health clinic?

Ms. ARONOVITZ. Right. Good question.

Senator DODD. There are a lot of them.

Ms. ARONOVITZ. There are a lot of questions. You are absolutely right.

Senator DODD. If you get information there, that is not protected by this regulation.

Ms. ARONOVITZ. The employer would at least have to have a fire wall between the activities—the employer could not use information from its health clinic to make decisions about promotions or other types of hiring decisions.

Senator DODD. So it is a gray area.

Ms. ARONOVITZ. Yes, I am sure it is, and I am sure there are a lot of questions like that.

Senator DODD. I presume you would think that would be an area we probably should close, in fact, if we are going to try to protect people's privacy records from unwarranted intrusion.

So my point here is that there are a number of areas that the regulations, despite their good intentions, do not cover.

Let me jump to a second point, and that is the preemption issue. There are a number of States which have enacted stronger legislation—at least, I believe they have—than what we are proposing here. I wonder if you could give us your views on that very quickly, and second, in your view, are there many State privacy laws in existence now that could be considered stricter, and have you seen any slowdown in States enacting legislation as a result of these regulations being implemented? Is that satisfying State legislative bodies, for instance, that there is no need for them to move into this area?

Ms. ARONOVITZ. That is very hard to tell. The regulation is so new, and the legislatures are just becoming organized again—although we hear that there is more interest in the States in privacy issues than there ever has been before—

Senator DODD. That is true.

Ms. ARONOVITZ [continuing]. Whether or not they would look at this rule and feel that this Federal floor were sufficient so they would not pursue their own regs. The groups that we spoke with are very concerned about the need to look at the Federal floor and then also the complexity of looking at individual State laws and making determinations as to whether they are more strict. Right now, they are doing it, but they do not have the Federal rule to contend with.

Ultimately, I think that privacy groups would feel very concerned about taking away more stringent rights that people have earned by virtue of living in a State with stricter rules. There are only four or five States that have comprehensive health privacy rules, although a lot of States have very specific and stringent rules for dealing with certain types of information, like information about HIV, pregnancy, or mental conditions.

Senator DODD. Senator Jeffords and I actually, in the crafting of that legislation, grandfathered States that had already enacted laws regarding privacy. That was one of the steps we took as a way of dealing with that issue politically.

I thank you very much.

The CHAIRMAN. Senator Murray.

Senator MURRAY. Thank you very much, Mr. Chairman, and thank you for having this hearing. I think this is an issue that is extremely important. Obviously, people's right to privacy is extremely important to them, and I certainly understand Senator Roberts' frustration with some of the regulations. But I also know that we have a lot of people who do not access the health care system because they are concerned that their privacy will be violated, and we do not want to discourage people from getting good health care. I think in particular of victims of domestic violence. Cases like that are obviously of deep concern to me. But I do think it is important that patients feel that their access to health care systems will give them some privacy, and I do think that the regulations are important and a great step forward. I am especially pleased with the protections for victims of domestic violence and also with the final regulation on protecting minors' access to confidential health care services. I think that those are extremely important.

Like others, I have concerns because some of the smaller health care providers are talking to us about the ability to comply within 24 months, and I wonder if you could talk to us about what a delay in implementation might mean, and how significantly would it weaken the legislation?

Ms. ARONOVITZ. The first thing I should say is that one of the principles in writing the legislation had to do with scalability, the acknowledgment that a large health system would have to comply in a much different way than, let us say, a small physicians practice. Whereas a small physicians practice might be able to use stickies and track things more manually or do things on a smaller scale, they would not necessarily have to buy a major new computer system, which in fact a larger system might have to do. So from that standpoint, there was that acknowledgment that small entities might not have to go through the same steps, but still, it clearly is going to be a burden for everyone to some extent.

In terms of the ultimate impact, one thing that is probably not widely understood is that the rule does not say that this rule needs to be fully implemented 2 years from the effective date. It says that this rule needs to be implemented on February 26, 2003. So there is a date certain there. What that means is that whenever this date is effective—and right now, that is February 26, 2001—all entities will need to comply.

We heard from a lot of groups that that 2-year time frame is unworkable. We have not really studied it. A lot of it has to do with individual entities and what they are going to be confronting. So we do not really have an opinion as to whether specific types of entities will be able to meet it, although we did speak to groups who understand a lot about technology and said that it is going to take every bit of that 2 years to just get the technological pieces in

place. It is definitely going to be a challenge, there is no doubt about it.

Senator MURRAY. Thank you.

I have one other question on the fact that the final regulation does not include any kind of private right of action or third party liability. I am concerned, for example, that if a patient is being treated for substance abuse, and the health care provider releases that information to that patient's employer, and the patient is fired from his job, unfortunately, under this regulation, the employee has no legal recourse in that kind of case. Obviously, the provider could be fined or penalized, but that does not do much for a person who has already lost his job.

Do you think that the lack of a private right of action undermines the strength of this regulation?

Ms. ARONOVITZ. Well, the privacy proponents would say it does, and that needs to be fixed in Federal legislation. People would still have a right of private action in their State courts, I assume—I am not a lawyer—but what we are talking about here is a specific right of private action with violation of this Federal rule.

HHS in developing the final rule felt that HIPAA did not give it the authority to include a right of private action, and therefore, legislative authority separately would have to be gotten.

Senator MURRAY. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. I believe you said 2001, and you meant 2003.

Ms. ARONOVITZ. The effective date is February 26, 2001, and then there is a 2-year implementation time frame, so even though the effective date of the rule is in a few days or a few weeks, the entities that are covered have 2 years to fully implement it. So you actually would not have to start getting the new consent until 2003, even though the rule is actually in effect.

The CHAIRMAN. All right. Thank you.

Senator DODD. But there is concern even about that 2-year period.

Ms. ARONOVITZ. Absolutely. There is a lot of concern about that.

Senator DODD. And that is an issue that I would love to have you take a look at at some point, because it is one that we are going to hear about from other witnesses here today. We all want to get this done, but we want to get it done right, and we would like to know how much more time is really necessary in terms of getting it done right—or whether the 2 years is adequate. I think we would like to know that.

The CHAIRMAN. Senator Clinton.

Senator CLINTON. Thank you, Mr. Chairman.

Thank you, Ms. Aronovitz, for an excellent report. I value the way in which you present your views and the evidence on which you base them.

Obviously, many of us believe that this privacy regulation is absolutely necessary and needs to be implemented as soon as is reasonably practicable, and that we could even go further in dealing with some of the areas that Senator Dodd and others have pointed out have not been adequately covered in this regulation.

There are two specific areas that I would like your advice on. The first area is the consent and disclosure provisions. Reading your testimony, it is clear that there were a number of groups, including the American Medical Association and the privacy advocates' groups, that did not think that we had adequately dealt with the consent issue, that there could be ways of obtaining consent when a person signed up for a health plan, when they first had a point of contact with any health care provider, that would satisfy the concerns of some of the plans about getting consent for the sharing of information.

Do you have any specific suggestions about how we could better balance this whole consent and disclosure issue, because that really goes to the heart of it. If someone gives informed consent, even if the consequences are such that they are surprised at how it has been utilized, that is a very different issue than if someone has not been asked for their consent, and the information is shared and disclosed.

Ms. ARONOVITZ. The underlying principle in the rule right now is that initial consent or consent is given for treatment, payment and health care operations. Ostensibly, when someone goes to a doctor, they are told through a privacy notice specifically what those activities include. Anything else really needs to have a separate authorization, and those are the kinds of instances that people are mostly worried about, where information would go to an employer or to a life insurance agent in terms of asking for life insurance. Any situation like that clearly has a separate authorization responsibility. And in fact we heard nothing to say that that is not prudent.

If anything, the groups were happy about the initial consent, because the proposed rule had more of a statutory consent or a perceived consent—you did not actually have to go and get consent. AMA and other advocacy groups said that right now, the way we practice medicine is that physicians get consent. AMA would like to also extend that to health plans, that they get consent, and they feel that they could do that through the enrollment process.

On the other hand, health plan groups we spoke with felt that it would be very unworkable to try to do that in that they do not always have an option as to whether to insure someone or not, and they would be in a dilemma if they did not have consent and therefore they tried to deny the insurance in those situations.

So it is somewhat problematic, although in my opinion, it is workable. It is a matter of working these things out.

Senator CLINTON. People are not only concerned about the disclosure of this information to either the general public or to someone whom they would not otherwise consent to having it disclosed, but they are also concerned about the marketing issues which arise out of this.

I understand health providers wanting to provide good information to their enrollees or trying to reach out and enlist more enrollees, but the idea of either mass mail marketing or telemarketing based on medical information is very troubling to a lot of people.

I know that there has been some resistance in that many health care providers want to go forward as broadly as possible, but again, do you have any suggestions about how we could balance patient

protection against unwanted marketing either in the regulation as it is currently written or in the way that it is enforced in the future?

Ms. ARONOVITZ. It is a very, very tough issue, because no matter what you do about marketing, whatever protections you have—and there are some right now in terms of giving the patient information about the source of the marketing—it is a very emotional issue for people. As many people who say that they do not want to have this kind of information used in that way and that it is a violation of their private information, there are arguments on the other side—and we heard a lot of them—that said that people very much would like to know when there is a new development or a new advance.

We are not really sure about the balance of people's feelings about that. The opt out, or the one free pass, is supposed to give people an opportunity to say that from now on, I do not want this information anymore. It is a very difficult process.

On the other hand, there is a provision where someone could request up front not to have this information at all. It is very difficult to do, though; it is not very well-known, and in fact there are questions as to whether it would actually work.

So it is a very troubling issue only from the standpoint that people have very strong feelings on this issue all across the board.

Senator CLINTON. Thank you.

The CHAIRMAN. Senator Harkin?

Senator HARKIN. Thank you, Mr. Chairman.

I will ask unanimous consent that my opening statement be made a part of the record.

The CHAIRMAN. Without objection.

Senator HARKIN. Thank you.

[The prepared statement of Senator Harkin follows:]

PREPARED STATEMENT OF SENATOR HARKIN

Thank you Chairman Jeffords and Senator Kennedy for holding this oversight hearing of the privacy regulation put forward by the Department of Health and Human Services. And although they're not testifying today, I want to thank HHS for moving us forward to protect the health privacy of all Americans.

I am concerned, however, by the Washington Post story from January 16 stating that there are provisions in the regulation that explicitly allow doctors, hospitals, health plans, and affiliated businesses to use people's private health care records for marketing and fund raising. This loophole shows us that in every aspect of this issue there are potential consequences that we may not immediately recognize.

The privacy issue is complex. It touches on just about every aspect of our nation's health care system. From health insurance to medical research to employee benefit programs to the oversight of Medicare and Medicaid, patients' medical records are involved. There is a delicate balance between protecting patients' rights to privacy, while at the same time ensuring that those who deliver our health care and those who work to improve it have access to the information they need.

Americans should feel confident that information about their health and health care will remain private. Patients shouldn't have

to worry that what they tell their doctors will become public information. Unfortunately, many people delay or even fail to seek needed treatment out of fear that their health privacy is not secure. Americans' confidence in our health care system is absolutely critical for it to run effectively.

Therefore, we must be vigilant and thoughtful and prepared to take corrective action for negative, but unforeseen, consequences. That is why I am pleased to participate in this oversight hearing to better understand the potential effects of the privacy regulation. Congress has responsibility to act to protect Americans' health records and ensure that patients can be confident in their health care system.

Senator HARKIN. Thank you again, Ms. Aronovitz, for your fine work.

I really have more of an observation than a question, and I cannot stay for the rest of the testimony, but the testimony of Ms. Janlori Goldman, who is director of the Health Privacy Project at Georgetown University's Institute for Healthcare Research and Policy, points out, for example, that a few months ago, a hacker downloaded medical records, health information, and Social Security numbers on more than 5,000 patients at the University of Washington Medical Center. Then, later on, in the testimony of Judith Lichtman, who is representing the National Partnership for Women and Families, she comments on the regulations, saying that there are not enough meaningful remedies for people when their privacy rights are violated.

Did you look at and examine the issue of remedies in your study? I understand the remedies provision to be basically that you file a complaint, HHS takes the complaint, and they may file several actions against the entity in question, but there is no right for the individual to go to court to seek remedies. Is that right?

Ms. ARONOVITZ. There is no right of private action in the Federal rule. Ostensibly, you would still be able to go to State court under some circumstances. But you are right, there is not a right of private action within the Federal rule. HHS felt that HIPAA itself did not provide that from a statutory framework.

Senator HARKIN. So that is the reason. HIPAA did not actually provide that they could do that in the regulations. Is that right?

Ms. ARONOVITZ. That is how HHS interprets HIPAA, that they would need separate legislative authority to include that in this rule.

Senator HARKIN. Finally, is it your understanding that this regulation is not affected by the Bush administration policy to postpone the effective date of all regulations recently published?

Ms. ARONOVITZ. Actually, we were looking to HHS to answer that. They would be the agency that would initiate any action in line with that memo. We have not heard either way in terms of what the administration is likely to do. There is an exception for regulations that were issued as the result of a congressional mandate, which this one is, but again, we do not know what interpretation HHS is going to take and how they are going to pursue that.

Senator HARKIN. So in your communications with HHS, they have not indicated one way or another whether they are going to open it up for further comments.

Ms. ARONOVITZ. Right. We have not heard what they are going to do in any regard in terms of opening this up or letting it become effective. We have not heard yet.

Senator HARKIN. Mr. Chairman, it is too bad—I wish we could have someone here from HHS to respond to that question. I would like to know what their intentions are in this regard as to whether they are going to try to reopen this or not.

Ms. ARONOVITZ. We would also, and we have not been able to hear yet.

Senator HARKIN. I hope we could ask them.

The CHAIRMAN. We will keep that in mind, Senator.

Senator HARKIN. Well, if we could ask them from the committee standpoint to respond to that and what their intentions are.

The CHAIRMAN. I will work with Senator Kennedy, and we will make sure we take care of that problem.

Senator HARKIN. All right, Mr. Chairman. Thank you.

The CHAIRMAN. Senator Reed?

Senator REED. Thank you very much, Mr. Chairman, and thank you, Ms. Aronovitz, for your testimony today.

The title of your written testimony is very appropriate—"Enhances Protection of Patient Records but Raises Practical Concerns." At the heart of all of our debates here is the tradeoff between privacy and convenience, and frankly, we want both, and that is the dilemma.

I want to raise just one area of concern, and that is the issue of pharmacies. As I understand the privacy regulations, they would be applicable to most pharmacies. And it is not uncommon in everyday life for someone to send someone else to pick up their prescription. As I understand it, there would have to be authorized consent to do that. We can all reflect on our own experience of being home ill and asking a neighbor to go out and pick up our prescription. That is routine and happens a million times a day.

To what extent do the regulations provide the flexibility to deal with this very practical issue?

Ms. ARONOVITZ. We spoke with several pharmacy groups that are very concerned about how they would fare with this regulation. There are provisions for indirect providers and direct providers. Pharmacists contend that most of the time, they have a direct treatment relationship with the patient, because they do more than just fill a prescription, obviously. They consider a person's complete medical history and make sure they are not taking any other drugs that would interact. There are many activities that pharmacists get involved in. So they would interpret this as being a direct provider of health care, and therefore, they feel that they would need separate consent.

They are very concerned about the situation that I mentioned in my oral statement, where the prescription is faxed to the drug-store, and a family member picks it up, and they never have an opportunity to give consent.

We brought this up with many similar types of situations with HHS in our exit conference with them, and HHS feels that there are a lot of these kinds of issues that need to be worked through. They do not have a definitive answer yet. They feel that they will have a panel of experts, and they will talk through these issues

and that the covered entities will figure out how to make this rule workable.

Senator REED. In that spirit, let me ask—and this is perhaps a question more directed at administrative law experts—what is the authority of HHS today to determine how the rule is perhaps overreaching or ineffective and to make changes? Is that something that they can do on their own volition?

Ms. ARONOVITZ. I am not an administrative procedural act expert at all, but my sense is that there would be a difference between doing something before February 26, 2001, when the rule becomes effective, and once it becomes effective. My sense is that it would be more difficult to make an amendment—you would have to go through a notice and comment period to do that—if your rule is effective. But I am not exactly sure what would need to happen before February 26 to change something that is currently in the rule.

Senator REED. In your outbriefing, was there any indication by HHS that they are—first, I presume from what you have said that they do realize that the nature of an amendment of this scope will engender lots of unanticipated difficulties—is it their sense that they are going to go forward and identify these issues and, if need be, post a proposed revision to the regulations for comment?

Ms. ARONOVITZ. What they have told us—and of course, this was just a few weeks after the regulation came into effect—is that they totally understand that there will be many, many inquiries and concerns. They have already received over 400 inquiries on their phone lines and websites, and most of those were procedural—am I covered, how do I get a copy of the rule, and things like that—but they are gearing up on their website. They said they will have a “Frequently Asked Questions” section on their website. We checked their website yesterday, and the frequently asked questions are not there yet, but they are in the process right now of compiling a lot of these concerns, and they say that they will deal with them internally and then work with the covered entities. They are going to spend the next 2 years trying to educate different groups and help them work out some of this thinking.

They did say that they have already visited 20 different organizations just since the rules passed, in terms of trying to explain this, so I think they understand the complexities and the challenges that they have ahead of them.

Senator REED. Just a final question—is the 2-year implementation period a date that was picked out by HHS, or is that something that they are required to do by law?

Ms. ARONOVITZ. My understanding is that that is set out in the HIPAA statutory framework.

Senator REED. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Wellstone.

Senator WELLSTONE. Thank you, Mr. Chairman.

I apologize, Ms. Aronovitz, for arriving late, but I want to thank you for your good work.

I would like to focus for a brief period on the mental health part of this. The Surgeon General issued a report in mid-December which I will say to my colleagues is very important. I will tell you that a lot of consumers and people around the country really took

heart. Some of them are parents whose children have died. In the case of Minnesota, in an organization called "SAVE," the leaders of that organization, Al and Marianne Klusner, lost two children to suicide—so this report is so important, because families are not only suffering through the tragedy of childhood suicide, but also are always fighting the stigma.

I wonder if you could give me your own analysis, based upon your look at these regulations as to how they affect mental health?

Ms. ARONOVITZ. There is a lot of interest in having higher and stricter standards for psychotherapy notes, and the rule does do that. You would need specific authorization for psychotherapy notes in almost every case—I am sure there are a few cases where you would not. So they are excluded from what is considered the rest of the protected health information that, for instance, an internal medicine physician would have.

In addition, there is a provision in the rule that a patient has the right to request a restriction of his or her medical information being passed on. The area where that comes up the most is in mental health. You could go to your physician and say, "I request that you not tell anybody that I am being treated for depression."

What we heard is that there is a very strong concern on the part of health care providers and health plans that that kind of information, although a patient would not want it to be shared, could ultimately have an effect on the well-being of that patient, because physicians really do need to know what other drugs someone is taking or how depression could enter into another illness. So there is a lot of debate about that, and in fact, the physician ultimately has the right to deny that request and say, "This is not in your best interest. We are not going to honor that request. We are going to make sure that your entire medical record stays intact."

When we talk to health privacy groups about that, they understand that that is the reality and that in some cases, it is in the patient's best interest; but they say that it is so important for that physician to have that conversation so the patient at least understands how his or her information will be used and why it is so important that that information stay intact.

On the other hand, when you talk to providers and health plans, they say that those conversations, which seem like a very positive and good thing, are very expensive. When your physicians are having to spend time talking to patients, as opposed to seeing other patients for diseases, they feel that that has got to be added into the calculus of the cost.

Those are the different sides of that argument, and that is really where the mental health issue arises most.

Senator WELLSTONE. Let me see if I can—and I am at a disadvantage, because I did not have the chance to hear your testimony—but you are saying that—can you frame that question for me again—you are saying that some of the managed care plans and others are saying that they need to have that information rather than having to take the time to talk to the patients at the time they are seeing them; is that what you are saying?

Ms. ARONOVITZ. No, no. It is not a matter of whether the physician ultimately gets the information, because I think there is an acceptance that if a physician makes a convincing argument, clearly,

they should have it. And actually, physicians under this rule could treat a patient and share information with other physicians for treatment purposes without getting separate consent.

The problem here is the tradeoff between having physicians and other people spend the time and the resources involved in assuring that patients understand their protections versus the time and money it costs to make those kinds of activities available. It is really a matter of cost is what we are hearing—not that it is not a good thing for physicians to be talking to their patients at all.

Senator WELLSTONE. So the tradeoff is whether or not the patients, the consumers, will be aware of the privacy issues and what their rights are and how much time the providers have to inform them of that; is that what you are saying?

Ms. ARONOVITZ. In this particular case, yes.

Senator WELLSTONE. I would think—and again, I am on the advocates' side on this question—but there has been so much stigma here and so much discrimination, I would think that we need to err on the side of making sure that the privacy of these men and women and younger people as well is protected, even if it takes a little extra time. But that is certainly my own position.

Ms. ARONOVITZ. I am sorry to interrupt, but I do think I could add one other thing that is important. That is, clearly, it is a policy discussion and one that has very strong feelings on both sides. But what physicians would also add is that they are responding this way in an environment or in a framework where physicians feel so incredibly overburdened by the rules and regulations that are required to be able to bill for their services that in their minds, this is one additional burden. So that is the context.

Senator WELLSTONE. As you were saying that, I was thinking of exactly the same context. Unfortunately, they are under a lot of pressure to see people and move them out and see other people and all the rest. I think this is a good example of where you can see some potential harm.

Thank you.

[The prepared statement of Senator Wellstone follows:]

PREPARED STATEMENT OF SENATOR WELLSTONE

I'd like to thank Senator Jeffords and Senator Kennedy and their staffs for arranging this hearing on an issue of vital importance to all Americans. I'd also like to commend former Secretary Shalala and her HHS staff for the prodigious amount of work involved in producing the final regulation and reviewing the voluminous comments regarding the privacy of individually identifiable health information.

As I said in January, 2000, I believe that Americans—almost uniformly—have certain expectations when it comes to their medical records. Americans expect that what they tell their doctors and other health professionals will be kept strictly confidential unless they consent otherwise. They expect that when they do consent to release information, only the minimal amount necessary will be disclosed to accomplish the purpose for which consent was given. Americans expect that confidential medical records will remain confidential during their lifetime and after their death.

I am pleased to see that my concerns, and those of most Americans, have been largely addressed. Although some changes in the regulations may be advisable, I look forward to their implementation on February 26, 2001, as scheduled. The American public has waited long enough for this fundamental right.

The CHAIRMAN. Thank you.

We have two other panels, but Senator Roberts has one burning question that he would like to pose.

Senator Roberts.

Senator ROBERTS. Mr. Chairman, thank you, with apologies to my colleagues and the rest of the panels. I am under strict orders that this is a follow-up question.

I think the goal is self-evident, and that is access. The distinguished Senator from Washington made that very clear, and I agree with her premise that it is how we do it and how we do not do it.

I am terribly worried about an unfunded mandate on top of many other unfunded mandates that will deny us the ability to get this job done. You talked about depression. I think that probably every hospital administrator in the country has depression after reading these regulations.

There is a rather incredulous statement here that says that HHS has factored in "administrative simplification provisions, saying that it will be a cost savings of \$29.9 billion over 10 years and that that will help offset the cost-covered entities of \$17.6 billion over 10 years that our health care providers will have to undergo."

But I think it is apples and oranges. If I were to tell a hospital administrator or any of the health care professionals in Kansas, "Do not worry, HHS will simplify all of your procedures and paperwork burdens and costs over \$30 billion in 10 years," I do not think they would hold their breath. I just do not think it is going to happen.

How is that addressed, if in fact it is a promise by HHS to simplify, to streamline, to computerize—and I am all for that, and I want to give them enough money to do it—but how does that take care of the problem of the hospital administrator in Abilene, KS to enforce all of these? It does not match up. I do not understand that.

Ms. ARONOVITZ. The cost estimates, I must say, are based on HHS' assumptions, and assumptions take many different forms. There are a lot of other cost estimates that are much different and much greater than that.

So, from the standpoint of \$30 billion being either savings or costs, again, that has to be suspect right off the top.

Senator ROBERTS. But the savings are in one item, and the costs are very evident in these regulations, and it does not—

Ms. ARONOVITZ. There is no doubt that these privacy regs will involve additional burden and cost on the part of all the covered entities and, actually, all of the players.

Senator ROBERTS. What about a little bill that somebody from Kansas introduced called the "Small Hospital Grants Program," which would allow a hospital at least to have the wherewithal to get the right people to do this and invest in the right equipment to get up-to-speed so we can get this job done the right way? I do not know who authored that bill; it seems to me it was a guy

named Roberts—but I would suggest to you that that might be part of the answer.

Senator WELLSTONE. I am opposed. [Laughter.]

Senator ROBERTS. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Ms. Aronovitz. As you can see, this is a very contentious area. So we appreciate your help, and we reserve the right to ask you questions.

Ms. ARONOVITZ. It would be my pleasure.

The CHAIRMAN. All right. Thank you very much.

Senator WELLSTONE. Thank you for your good work.

The CHAIRMAN. Our next panel includes Ms. Janlori Goldman, director of the Health Privacy Project, Institute for Healthcare Research and Policy at Georgetown University. Ms. Goldman created the Project, which is dedicated to ensuring privacy protection in the health care environment. Her professional experience includes service as a staff attorney and director of the Privacy and Technology Project of the American Civil Liberties Union, where she led the effort to enact the Video Privacy Protection Act. She has testified before Congress and served on numerous commissions and has written extensively on health privacy.

Thank you for appearing before the committee, Ms. Goldman. It is a pleasure to have you with us today.

Our next witness will be Ms. Jane F. Greenman, who will be testifying on behalf of the American Benefits Counsel. Ms. Greenman is deputy general counsel of human resources at Honeywell International, Incorporated, in Morristown, NJ. A graduate of Cornell and New York University Law School, Ms. Greenman was partner and chair of the employee benefits department of Hughes, Hubbard and Reed in New York. In addition, she has been on the faculties of NYU, Brooklyn, and Hofstra Law Schools, teaching courses in employee benefits, pension rights, and legal writing.

Ms. Greenman, it is nice to have you here with us this morning.

Ms. GREENMAN. Thank you.

The CHAIRMAN. And our final witness on this panel will be Mr. John P. Houston, representing the American Hospital Association. Mr. Houston is a director in the Information Services Division of the UPMC Health System in Pittsburgh. He has tracked the Health Insurance Portability and Accountability Act, fondly known as HIPAA, at UPMC Health System, and he has spoken about HIPAA in a variety of forums. He graduated from the University of Pittsburgh and Duquesne University School of Law.

It is nice to have you with us again, Mr. Houston.

We will start with Ms. Goldman. Please proceed.

STATEMENTS OF JANLORI GOLDMAN, DIRECTOR, HEALTH PRIVACY PROJECT, INSTITUTE FOR HEALTHCARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY, WASHINGTON, DC; JANE F. GREENMAN, DEPUTY GENERAL COUNSEL FOR HUMAN RESOURCES, HONEYWELL INTERNATIONAL, INCORPORATED, MORRISTOWN, NJ, ON BEHALF OF THE AMERICAN BENEFITS COUNSEL; AND JOHN P. HOUSTON, DIRECTOR, PRODUCTION SERVICES, DATA SECURITY OFFICER, AND ASSISTANT COUNSEL, UPMC HEALTH SYSTEM, PITTSBURGH, PA, ON BEHALF OF THE AMERICAN HOSPITAL ASSOCIATION

Ms. GOLDMAN. Thank you very much, Mr. Chairman, Senator Dodd, and Senator Wellstone. I very much appreciate the chance to be here with you today, and I also want to thank you for not putting me last on the agenda this morning.

I want to just give you some very quick background about the Health Privacy Project. One thing that we have been doing for the last few years, really triggered by the passage of the Portability Act, was to look at the impact of privacy in the health care setting and to understand how the lack of privacy affects the quality of care that people get and whether they are willing to even seek care at all.

What we have found through a number of empirical studies that go beyond anecdotes is that when people are worried about whether their employers will get access to information, or if information will be divulged to family members or to their communities, they withdraw. They do not share fully; they sometimes give inaccurate information to their doctors; they may pay out of pocket for care to which they are entitled for reimbursement. Sometimes they stay away altogether.

So not only are they putting themselves at risk for untreated and undiagnosed conditions, but they are also affecting the quality of the information that our Nation's researchers and public health officials rely on, that hospitals rely on in doing outcome studies. All of that information, if there is a piece missing, if there is something that is inaccurate, if people are staying away, we do not have reliable data to do work to improve the health of our communities.

So we believe that it is very important that privacy be at the center of all of our health care activities so that we can improve care on an individual and a community level.

We know, obviously, that Congress and this committee in particular acknowledged the urgency of acting in this area, given that we did not have a Federal law, and built into HIPAA this series of time lines, deadlines, for either the Congress or the administration to act. And when the administration issued a draft of privacy regulations over a year ago, it left ample time for public comment. In fact, the comment period was extended in part because of the requests from the consumer community and from the industry, saying give us a chance to really express our views on this draft. So the comment period was extended. You had 52,000 comments that the administration really sifted through, and I think that at least up until today, there has been fairly good agreement on the part of both the industry and the consumer groups and the provider groups that the administration did a really fine job of taking into

account all of those comments to try to craft a strong privacy rule but also one that is workable in the health care setting. That was their goal, and I think they have gone a very long way toward achieving that.

What I want to do very quickly—our written statement is exhaustive in terms of giving you a summary of the regulation—you hear very often, and I am sure you will hear this morning, that the regulation is very complicated and very vague. We actually do not think it is as vague and complicated as some would like to hold out, and what we have tried to do is to break it down and put together a summary for you that is attached to our testimony. But let me quickly go through the major provisions in the regulation.

It covers directly health care providers and health plans that electronically transmit health data. It gives individual consumers for the first time ever notice of how their information will be used. When they go to a doctor or they enroll in a health plan, it gives people a chance to see their own medical records—a Federal right that they do not currently have in many States in this country.

And it creates some limits on disclosure, and I just want to clarify what those limits are. Health care providers now, under the regulations, in response to concerns that the AMA raised, must get consent before they can use information. However, they can say to their patients, "I must get your consent in order to treat you." Once they get that consent, they can share information freely with other health care providers. There are no limits on how they can share that information. The "minimum necessary" requirement does not apply to health care providers to treat people and to take care of them; that information can be freely shared in a health care setting.

Health plans and health care clearing houses may get authorization. They are not required under the regulation to get authorization when people enroll in a plan. They may get it if they choose.

Another provision in the regulation that we think is important is that health plans and health care providers will not be able to disclose information to employers without consent. Now, obviously, if an employer is wearing the hat of a health care provider or a health plan, they are covered in that capacity under the regulation. But where it is the personnel side of the company, they may not receive protected health information under the regulations. That is a critical provision and goes to the heart of what most people in this country care about, which is trying to maintain some degree of privacy and dignity in their work environment.

I think it is also important to note in terms of discrimination that the privacy regulations are really the missing piece of the Americans with Disabilities Act, that really give people the opportunity to say to their employers, "I do not even want you to know this about me." And in addition, if you do know it, you cannot act on it in a discriminatory fashion. I think it is an important provision there.

Business associates—every, single hospital health plan in this country, I would hope, engages in some contractual relationship before they share information on patients. I would hope that that is already good and responsible business practice. What the regulation does is require that a contract be entered into with a business

associate so that there is a chain of trust, and protections will follow the data when they leave the covered entity.

In the research area, I think the major provision is that the regulation extends the scope of protection to privately-funded research. It takes the rules that are currently in place at the Federal level for federally-funded research, and it says that if you are engaged in privately-funded research, you also need to be accountable, you also need to go through an institutional review board or a privacy board to make sure that privacy is being protected.

The law enforcement area is an area where many of us thought the administration could have done better, but it is certainly much better than what we have now, which is no protection. The administration has required that there be some form of legal process before health plans and health care providers can share information with law enforcement. We would like to see those improved.

In the penalties—you have heard a lot about this already—there are civil and criminal penalties, again, mandated under HIPAA, that will apply if the rule is violated, if the Office of Civil Rights at HHS is aware of it, and they can mount an enforcement action. But the lack of a private right of action I think is a serious impediment to accountability and a serious impediment to making this regulation real in people's lives.

On preemption, again, HIPAA and this committee, this Congress, required that stronger State laws be in effect; that if the regulation came out, it had to leave in place stronger laws.

Our Project did a survey of State confidentiality statutes—I know that many of you have seen this—and what it says is that very few States have comprehensive law in this area, so the enactment of a regulation is going to provide substantial uniformity. You will no longer have to worry as much about the 50 different State laws, because the weaker laws will fall out, and those more condition-specific or disease-specific laws that the States have passed—many of you have them in your States—that deal with HIV or mental health or abuse and neglect, that this regulation does not even begin to address, those laws will continue to be in place. So I think that substantial uniformity will be achieved.

I ask, please, that a letter that we have provided be submitted into the record. Yesterday, we organized 39 groups who signed a letter to Secretary Thompson, asking that under the Card memo, the memo from Chief of Staff Andrew Card, the exception to the moratorium on recently-issued regulations that applies to those regulations issued pursuant to a statutory mandate, that these privacy regulations be considered part of that exception. It seems clearly within the language of the exception.

And we also take note that we do not think that a delay is in order. We believe that the Secretary of HHS has ample authority to respond to concerns where there are issues around technical compliance. He has full legal authority to respond to those concerns on a case-by-case basis as they arise.

The CHAIRMAN. Without objection, it will be included.

[The letter referred to follows:]

CONSUMER COALITION FOR HEALTH PRIVACY,
2233 WISCONSIN AVE., NW,
Washington, DC,
February 7, 2001.

The Honorable Tommy G. Thompson, Secretary,
U.S. Department of Health and Human Services,
200 Independence Ave., SW,
Washington, DC.

*The Honorable Tommy G. Thompson, Secretary,
U.S. Department of Health and Human Services,
200 Independence Avenue, SW,
Washington, D.C.*

DEAR MR. SECRETARY: We, the undersigned, are writing to express our strong support for the full and timely implementation of the final rule on medical privacy that was issued by the Department on December 20, 2000, pursuant to a statutory deadline. As such, we request that you notify the Director of OMB that the privacy regulation is exempt from the moratorium imposed by the Regulatory Review Plan, as outlined in the January 20th memorandum.

As you know, the privacy rule is one of three regulations mandated by the 1996 Health Insurance Portability and Accountability Act (HIPAA). HIPAA itself includes a timeline for the promulgation of regulations so that all three regulations—transaction standards, privacy, and security—may be implemented in roughly the same time frame. The transaction standards, which encourage the dissemination of health information electronically, are already in effect, so it is imperative that the privacy rule takes effect as scheduled. Preliminary cost analysis shows that there, will ultimately be a cost savings when the regulations are implemented together.

The draft privacy regulation was published in the Federal Register on November 3, 1999. At the request of industry and consumer groups, the public comment period was extended. There were more than 52,000 comments on the draft regulation. The Department was careful to respond to many concerns, and both industry and consumer groups have noted favorable changes in the final regulation. The rule is workable, scalable, and fair to the numerous parties that will be affected by it. Furthermore, the statute creates a mechanism for you to respond to unforeseen problems that may arise once covered entities begin to implement this regulation.

We understand that various members of the health care industry are urging you to delay implementation of this rule. A decision to delay the implementation of this rule would violate the integrity of the rulemaking process and is unjustified on the merits. Americans have already waited too long for federal rules to protect the privacy of their medical records—People's health care is at stake—we urge you to adhere to the legally mandated timeline.

Respectfully,

AIDS Action, American Association for Marriage and Family Therapy, American Civil Liberties Union, American Counseling Association, American Federation of State, County and Municipal Employees, American Nurses Association, The Arc of the United States, Bazelon Center for Mental Health Law, Center for Reproductive Law and Policy, Center for Women Policy Studies, Citizen Action of New York, Consortium for Citizens with Disabilities Health Task Force, Consortium for Citizens with Disabilities Rights Task Force, Consumer Action, Cystinosis Foundation, Families USA, Family Violence Prevention Fund, Federation of Families for Children's Mental Health, Gay Men's Health Crisis, Genetic Alliance, Hadassah, Health Privacy Project, Housing Works, Human Rights Campaign, National Alliance for the Mentally III, National Association of Developmental Disabilities Councils, National Association of People with AIDS, National Consumers League, National Health Law Program, Inc., National Minority AIDS Council, National Multiple Sclerosis Society, National Organization for Rare Disorders, National Partnership for Women & Families, National Therapeutic Recreation Society, New Yorkers for Accessible Health Coverage, Project Inform, San Francisco AIDS Foundation, and Title II Community AIDS National Network

Ms. GOLDMAN. Thank you, Mr. Chairman.

The four major changes that we would like to see are divided into two areas. One is those changes that HHS has the legal authority to pursue because it is part of the mandate from HIPAA, that is, areas where they have legal authority to actually affect the regulation. The other two are areas where only the Congress can act. The two areas where we think both the administration and the

Congress can act are in the law enforcement area, to tighten those provisions so that a neutral magistrate should always be looking at whatever legal process issued, and it cannot just issue out of a law enforcement office. We also think that the marketing and fund raising provisions should be tightened. I know there is a lot of discussion about that as well.

We are not suggesting an absolute bar to disclosure in use of information. We just think that people should be able to say up front if they want to receive a marketing letter, if they want to receive fund raising material. They should be able to say, "Please give that to me," or "I do not opt out of receiving that material." That is the tightening that we are looking for here.

In the areas that we think Congress needs to address, there are two. One is to create a private right of action to make this really enforceable by individuals and to look at the scope of the regulation so that the issue of liability, the issue of having only the covered entities really responsible for overseeing this rule, is more fairly apportioned in that there are other groups that do directly collect and use information—employers, for instance, pharmaceutical companies, life insurers—who should, I think, be more directly regulated to make this a fair rule.

In conclusion, Americans should be proud of what Congress set in motion with HIPAA. Now, we should all turn our focus and our resources to implementation. Efforts to weaken or withdraw the new law are, we believe, an hysterical reaction to the new regulation. It is no matter to some of these groups that it is nearly a decade in the making—Congress has been looking at this issue for over a decade. There have been many bipartisan proposals out of this committee, many of which are similar to what we see in the regulations, and the law is the product of a formal and exhaustive rulemaking process.

The American people deserve more from their health care institutions. Protecting privacy is a fundamental patient right that is central to improving care and breaking down barriers to access to care. Instead of focusing on delay, we urge Congress to move ahead to finish the job that you started on HIPAA.

As many of you know, we have seen astounding breakthroughs in genetics and in Internet-based health care which cannot go forward without the full trust and confidence of the American people, and assurances that their privacy will be first, that privacy protections will go hand-in-hand. The administrative simplification regulations are actually part of all of this—privacy; the transaction standards were intended by this committee and by Congress to be implemented together. That is why, when you hear about ultimate cost savings, it is because there was the intention that they should be implemented at the same time so that we have the privacy protections as we are creating electronic health information systems.

I very much appreciate the chance to be here today, and I look forward to any questions that you might have.

The CHAIRMAN. Thank you.

[The prepared statement of Ms. Goldman follows:]

PREPARED STATEMENT OF JANLORI GOLDMAN

Members of the Senate Committee on Health, Education, Labor, and Pensions: As the Director of the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy, I very much appreciate the invitation to testify before you today on the final medical privacy regulations.

OVERVIEW OF HPP

The Health Privacy Project's mission is to press for strong, workable privacy protections in the health care arena, with the goal of promoting increased access to care and improved quality of care. The Project conducts research and analysis on a wide range of health privacy issues. Recent Project publications include: *Best Principles for Health Privacy*, (1999) which reflects the common ground achieved by a working group of diverse health care stakeholders; *The State of Health Privacy*, (1999) the only comprehensive compilation of state health privacy statutes; *Confidentiality and Research*, (2000) commissioned by the National Bioethics Advisory Commission; *Privacy and Health Websites*, which found that the privacy policies and practices of 19 out of 21 sites were inadequate and misleading; and "Virtually Exposed: Privacy and E-Health," 2000, published in *Health Affairs*.

In addition, the Project staffs the Consumer Coalition for Health Privacy, comprised of over 100 of the major disability rights, disease, labor, and consumer advocates, as well as health care provider groups. The Coalition's Steering Committee includes AARP, American Nurses Association, Bazelon Center for Mental Health Law, National Association of People with AIDS, Genetic Alliance, Multiple Sclerosis Society, and National Partnership for Women and Families.

THE GENESIS OF THE REGULATIONS

The new federal health privacy regulations are a major victory for all health care consumers. Each one of us will benefit from these rules in some way. The rules represent a significant and decisive step towards restoring public trust in our nation's health care system. Not only is it the most sweeping privacy law in U.S. history, it begins to fill a most troubling vacuum in federal law. The regulation sets in place a sorely-needed framework and a baseline on which to build. Much of the regulation's unfinished business is due to the legal constraints imposed on the Department of Health and Human Services by Congress in its delegation of authority in HIPAA. At this juncture, it is imperative that Congress act to plug the gaps and strengthen the weaknesses in the rule.

In fact, it was the Congress that imposed on HHS the legal duty to issue health privacy regulations. In the 1996 Health Insurance Portability and Accountability Act, Congress imposed a deadline on itself to enact a comprehensive health privacy law within three years. Failure to meet the deadline triggered the requirement for HHS to promulgate rules in this area by 2000. Many bills were introduced, including by many members of this Committee. Some were bi-partisan, others were not. Some were favored by consumer advocates, others by health plans. Numerous hearings were held in both the House and this Committee, but not a single bill saw a mark-up. Achieving consensus on health privacy rules is not a simple task.

Pursuant to its mandate, HHS issued draft regulations in November 1999. In response to requests from industry representatives and consumer advocates, the Department extended the formal comment period to allow sufficient time to respond to the proposal. Of the 52,000 comments eventually submitted, more than half came from consumers and their representatives. The final regulation incorporates a number of the key changes sought by consumer groups, as well as many of the changes urged by health care providers, health plans, clearing houses, researchers, and others operating in the health care arena. It appears HHS was striving to craft a strong and workable privacy law.

It is important to note here that the privacy rule is one of three regulations mandated in the section of HIPAA known as "Administrative Simplification." The other rules address establishing uniform transaction standards for health care, and security rules to safeguard the data. Congress intended this package of regulations to be implemented together so that as information systems and practices are standardized, so too will privacy and security measures be built-in. The policy goal was to assure the public that as their most sensitive personal information was being computerized and adapted to be shared instantly and cheaply, enforceable privacy rules were being implemented up-front.

PRIVACY IS CENTRAL VALUE IN HEALTH CARE

In HIPAA's privacy mandate, Congress recognized that Americans are increasingly concerned about the loss of privacy in every-day life, and especially for their health information. The lack of privacy has led people to withdraw from full participation in their own health care because they are afraid their most sensitive health records will fall into the wrong hands, and lead to discrimination, loss of benefits, stigma, and unwanted exposure. One out of every six people engages in some form of privacy-protective behavior to shield themselves from the misuse of their health information, including withholding information, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and—in the worst cases—avoiding care altogether. (Survey conducted by Princeton Survey Research Associates for the California Health Care Association, 1999)

Unfortunately, peoples' fears are warranted. Medical privacy breaches are reported with increasing frequency by the media. To highlight a few—Terri Seargent was fired from her job after her employer learned that she had been diagnosed with a genetic disorder that would require expensive treatment. Terri was a valued employee who received a positive review and a raise just before her discharge from the company. A recent EEOC investigation determined that the employer fired Terri because of her disability.

A few months ago, a hacker downloaded medical records, health information, and social security numbers on more than 5,000 patients at the University of Washington Medical Center. The University conceded that its privacy and security safeguards were not adequate.

Annette W. and her husband were involved in a difficult and contentious divorce. In the midst of their separation, Annette instructed her pharmacy not to disclose any of her medical information to her estranged husband. Just one day later, the pharmacist gave Annette's husband a list of all her prescription drugs. Armed with this information, her husband embarked on a campaign to label her a drug user. He sent information to friends and family, to the Department of Motor Vehicles, and threatened to have her children taken away.

Years ago, Ben Walker and his wife came to Congress and to this Committee to tell their story. Ben had worked for the FBI for 30 years, but was forced into early retirement after his employer learned that he had sought mental health treatment. The FBI got hold of Ben's prescription drug records when the Bureau was investigating his therapist for fraud. In turn, the FBI targeted Ben as an unfit employee and stripped him of many of his duties, even though he was later found fit for employment. Ben and his wife testified that he would never have sought treatment had he believed his medical records would be used against him.

In the absence of a federal health privacy law such as the one we have now, these people suffered job loss, loss of dignity, discrimination, and stigma. And had they acted on their fears and withdrawn from full participation in their own care—as nearly 20% of people do—they would have put themselves at risk for undiagnosed and untreated conditions. In the absence of a law, people have faced the untenable choice of shielding themselves from unwanted exposure, or sharing openly with their health care providers.

SUMMARY OF REGULATIONS

Key provisions of the health privacy regulation are highlighted below. Attached to this statement is a more detailed, comprehensive summary of the rule.

Scope: The regulation applies all health care providers, health plans, and clearing houses (entities that process and transmit claims data) that transmit health information in electronic form, and covers identifiable health information in electronic and paper records, as well as oral communications. Due to the constraints imposed by HIPAA, the law does not directly cover employers, life insurers, pharmaceutical companies, and others. Instead, the rule establishes a chain of trust requirement, binding entities that receive identifiable health information from a covered entity to a contractual arrangement.

Access: People have the right to see and copy their own medical records. Most states do not currently grant people such broad access.

Limits on Disclosure: The regulation restricts access to and disclosure of health information. Of particular importance to patients and providers, health care providers must obtain patient consent for disclosures relating to treatment, payment and health care operations. However, we believe the sections on marketing and fund-raising are fundamentally flawed in allowing "one free pass" before first giving people the chance to opt-out of receiving such communications.

Employers: Employers are barred from receiving "protected health information" except for specific functions related to providing and paying for health care. Employers must establish a firewall between the health care division and employees who make decisions about employment. The rules are a powerful new tool to stop workplace discrimination. However, due to constraints imposed by HIPAA, employers that collect health information directly from employees (and not in their capacity as providers, plans or clearing houses) fall outside the scope of the privacy rule. cause the regulation can not directly cover employers. This gap should be closed.

Law Enforcement: Health care providers and plans are prohibited from releasing patient data to federal, state, or local law enforcement without some form of legal process, including a warrant, court order or administrative subpoena. But the legal process requirements should be strengthened to require a higher Fourth- Amendment standard and review by a neutral magistrate.

Research: All research, whether publicly or privately funded, must be overseen by either an Institutional Review Board (IRB) or Privacy Board if the researcher seeks a waiver of informed consent.

Penalties: Health care providers, health plans, and clearing houses are subject to civil and criminal penalties (up to \$250,000/year and 10 years in jail) for violating the law. The Office of Civil Rights at HHS is charged with overseeing the law and imposing penalties where appropriate. But, HIPAA constrained the Secretary from including a private right of action for individuals to sue for violations of the law. Congress should act to give people the ability to seek redress directly if their rights are violated

Preemption: As required in HIPAA, the federal regulation does not preempt or override stronger state law. Instead, the rules establish a baseline of protections, above which the states may go to better protect their citizens. A 1999 report issued by the Health Privacy Project demonstrated that such a baseline is sorely needed.

Cost: Government estimates that the cost associated with implementing the privacy regulation (approximately \$17 billion over 5 years) will be greatly offset by the cost savings associated with implementing HIPAA's transaction standards (approximately \$29 billion saved over 5 years). Again, if implemented together as contemplated by Congress, consumers will benefit, health care organizations will benefit, and the health of our communities will benefit.

CONCLUSION

In conclusion, Americans should be proud by what Congress set in motion with HIPAA. Health care providers, plans, and clearing houses should focus their resources in the coming years on implementing the HIPAA regulations, thereby improving health care quality and access, while also protecting privacy. At the same time, we urge this Congress to:

1. broaden HIPAA's scope to directly cover other entities that collect and use personal health information;
2. require consumer consent before medical information can be used for marketing and fund-raising;
3. strengthen the limits on law enforcement access to medical records; and
4. equip people with the right to go to court if their privacy is violated under the law.

We look forward to continued progress on health privacy. Our health care system has changed dramatically in the last few years, bringing with it both promise and perils. We have mapped the human genome, but people are afraid to get tested. The Internet can deliver cutting edge research and health care services, but people are unwilling to trust their most sensitive information in cyberspace. We will never fully reap the benefits of these astounding breakthroughs until privacy is woven into the fabric of our nation's health care system.

The CHAIRMAN. Ms. Greenman, please proceed.

Ms. GREENMAN. Good morning, Mr. Chairman, and thank you for this opportunity to testify.

As you know, I am Jane Greenman, deputy general counsel for human resources with Honeywell, and I am here today representing the American Benefits Council, a trade association representing principally Fortune 500 companies.

Collectively, our Council's members sponsor directly or provide services to employee benefit plans that cover more than 100 million Americans. The new HHS privacy rules are sweeping in their scope

and will present many significant implementation challenges. We sincerely appreciate your leadership and your continuing efforts to develop a workable and effective framework for national safeguards in this area.

Overall, we share the objectives which these regulations aim to achieve, and we agree that an individual's privacy concerning medical records and other personal health information should be respected and protected. But we believe that there is significant opportunity for improvement in these rules and that they should be re-proposed to allow for public comment on many of the changes that were made between the proposed rules and the final rules.

Specifically, Mr. Chairman, we recommend that this committee direct the new Secretary of HHS to seek additional public comment as to how the regulations could be simplified, clarified, and made less burdensome; to report to Congress on his findings and recommendations and to propose appropriate actions, including, perhaps, seeking additional legislative authority, and certainly the issuance of a re-proposed regulation.

During this time of review, in order to avoid unnecessary confusion and expense, we would urge that the current regulations be withdrawn or suspended.

Just to briefly summarize some of the key issues that arise under these regulations for employers, the American Benefits Council believes that Federal privacy rules should establish a true national uniform standard. Large employers like Honeywell find uniformity to be critical to meeting our commitment to the equitable treatment of employees, regardless of where they live or work or obtain their health care services.

We recognize that HHS is limited in its ability to create uniform national privacy standards, but we also believe that it is not realistic or desirable to place the burden on each regulated entity to try to sort out whether Federal or State standards apply.

Accordingly, we would urge Congress to direct the Department to publish its determination of which existing laws and regulations would not be preempted before employers and others have to comply with State standards. We believe that it is the Department's continuing responsibility to review State laws and publish notices about their effect relative to the Federal rules.

It is noteworthy in this regard that HHS decided not to issue advisory opinions or to issue opinions as to whether a given State law applies because of what they characterized as the burden of undertaking such an exercise and the uncertainty as to whether courts would honor their determinations. Imagine if it is too burdensome for HHS how burdensome it would be for individual employers.

There should also be a "safe harbor" until a Federal determination is made for many enforcement actions or penalties if organizations are either in compliance or are making a good faith effort to comply with a new State requirement.

The consent and authorization provisions in the HHS rules raise serious procedural and substantive issues. During the proposed rule stage, the Department had adopted the concept that prior individual approval was not necessary and indeed not permitted as long as the information was used for specified purposes, such as payment, treatment, and health care operations. In the final rule,

the Department retreated from its original position and has now required health care providers to obtain individual consent forms.

We believe that the public comment process would have aired many of the costs and disadvantages of this new rule and enabled the more balanced rule to be developed.

The regulations also adopt an ambiguous standard that covered entities may not use or disclose more than the minimum amount of information necessary for a particular purpose. However, they do not define "minimum necessity," what would constitute "minimum necessary" information, or provide any guidance as to how an employer or another covered entity would determine minimum necessity.

We would recommend that instead of "minimum necessary" or "minimum necessity" as the operative standard, a "rule of reason" standard based on a prudent professional's determination of the information needed to accomplish an intended purpose be substituted.

Again, the final rule imposes entirely new obligations on the sponsors of group health plans that are difficult to interpret and, we believe, may not achieve their intended purpose. For example, they fail to adequately address the administrative realities of many large employers who have self-insured plans. They call for adequate separate between the group health plan employees and other employees of a plan sponsor. This fire wall concept is simply not feasible in many instances, and this problem is more acute for small employers, where the individual employee may wear many hats within the company.

Let me conclude by expressing my support for the basic principles set forth in the regulations. But I would urge the Department to issue regulations that provide national uniformity, simple, clearly understandable processes and procedures and, in operation, provide model notices and forms that will avoid abuse or misuse of information but will not add burdens and bureaucracy to health care delivery and administration.

I thank you, Mr. Chairman, and members of the committee for the opportunity to share our views with you.

The CHAIRMAN. Thank you, Ms. Greenman.

[The prepared statement of Ms. Greenman follows:]

PREPARED STATEMENT OF JANE F. GREENMAN

Good morning, and thank you, Mr. Chairman, for the opportunity to appear today to present our views on the new regulations by the Department of Health and Human Services (HHS) on the privacy of health care information. I am Jane F. Greenman, and I am the Deputy General Counsel for Human Resources with Honeywell. I am here today representing the American Benefits Council where Honeywell serves on the Board of Directors. The American Benefits Council is a trade association representing principally Fortune 500 companies and other organizations that assist employers of all sizes in providing health care, retirement and other benefits to employees. Collectively, the Council's members either directly sponsor or provide services to employee benefit plans that cover more than 100 million Americans.

I also want to thank you, Mr. Chairman, for these timely hearings on this important issue. The new HHS privacy rules are sweeping in their scope and will present many significant implementation challenges. Before employers and other organizations begin to take the next steps to comply with these highly detailed new rules, there will be keen interest in the response this Committee has to the HHS standards. We sincerely appreciate your leadership in setting the direction for federal

health information privacy standards and your continuing efforts to develop a workable and effective framework for national safeguards in this area.

RECOMMENDED ACTION BY CONGRESS

Overall, we share the objectives these regulations aim to achieve. We agree that an individual's privacy concerning their medical records and other personal health information should be both respected and protected. However, as I will discuss in the remainder of my statement, we believe that there is opportunity for significant improvement in the privacy rules issued during the final days of the previous Administration. Now is the time, in our opinion, for the new Administration to examine these regulations to see how they might be clarified and simplified before these requirements begin to be put in place.

Specifically, we recommend, Mr. Chairman, that this Committee direct the new Secretary of Health and Human Services to:

1. Seek additional public comment on how the regulations could be simplified, clarified or made less burdensome,
2. Report to Congress on his findings and recommendations on what modifications should be made to the privacy standards issued by the former Administration in December 2000, and
3. Propose appropriate actions—including any additional legislative authority and/or the issuance of a revised regulation - to achieve the Secretary's recommended improvements.

During the time of this review, we would also urge the current regulations be withdrawn or suspended so it is clear that implementation actions should await the Secretary's review.

SUMMARY OF KEY ISSUES FOR EMPLOYERS

We believe more work is needed to strike the appropriate balance between the desire for firm safeguards for individual privacy and the need for clear, workable standards that can be implemented consistently and efficiently in our complex health care system. We are now at the very beginning of the far-reaching compliance process affecting—at a minimum—every hospital, health care professional, health insurer, pharmaceutical company and most of the nations employers. It would be a major achievement to successfully implement these rules in even one of these important sectors. But we are equally certain successful compliance with these regulations throughout our health care system is not possible given the rules' current complexity and ambiguity.

In the remainder of my statement, I highlight four of our major concerns with the HHS privacy rules where we believe improvements should be made.

First, we recommend strongly that federal privacy rules should establish a true nationally uniform standard as the only way to achieve clearly understood, workable requirements and a single enforcement scheme. Second, the consent and authorization provisions in the HHS rules raise serious procedural and substantive problems because they were not subject to prior public comment where corrections could have been made and because they could actually result in harming patients in their present form. Third, the regulations would allow only "minimally necessary" information to be obtained for any particular purpose, an ambiguous standard that the rules nonetheless assume can be implemented as if there were a clear bright line basis to determine minimal necessity. Finally, the rules place new requirements on employers as plan sponsors that are both difficult to understand and, in many cases, could not possibly achieve the desired objective of limiting the use and disclosure of health information for group health plan purposes.

This Committee should be aware that although the rules are well-intended, they create burdensome requirements that will frustrate the effective, timely and cost effective delivery of health services. Protection of privacy rights can certainly be achieved with far less invasive and bureaucratic standards.

THE IMPORTANCE OF UNIFORM NATIONAL STANDARDS

The American Benefits Council has consistently supported the establishment of uniform national standards as the only way to achieve workable, understandable protections for health information and a single enforcement scheme. Indeed, the most compelling case for a nationally uniform standard is presented by the fact that information in today's technology-driven health care field is transmitted with a single click, without regard to any state boundaries. The multiplicity of individual state privacy laws, however well-intentioned, lead in the aggregate to an unnecessarily complex regulatory scheme creating confusion for both regulated entities and

consumers alike. Uniformity can enable real strides to educate consumers about their rights, allow organizations to replicate proven effective practices, and permit clear and consistent interpretation of the inevitable regulatory "gray areas" that are sure to arise as the new standards begin to be implemented.

For large employers such as Honeywell, uniformity in an area such as health information privacy is critical to meet our commitment to the equitable treatment of our employees regardless of the state where they may live, work or obtain their health care services. We also try to constantly improve our health plan administration to benefit our employees and their dependents and to achieve greater economies of scale. Attempts to comply with inconsistent state privacy standards will increase employers' compliance burdens, frustrate their ability to set consistent corporate privacy protection policies, and limit their ability to communicate effectively to their employees and business partners about their practices.

We recognize the statutory authority provided by Congress as part of the Health Insurance Portability and Accountability Act (HIPAA) limited the ability of HHS to achieve nationally uniform privacy standards. However, we also believe it is not realistic or desirable to place the burden on each regulated organization—or each individual whom the regulations seek to protect—to sort out whether federal or state standards apply in particular circumstances. Not only is this process going to be an arduous and expensive task, it is also certain to lead to inconsistent interpretations and expensive litigation over differing interpretations of the limits of overlapping federal and state requirements. No company has the resources to get this job done right; assurance of being in compliance with these rules would be impossible even for the most conscientious companies.

We continue to strongly favor a uniform federal framework for health information privacy standards and we recognize that to achieve that objective, further legislative action by Congress is needed. However, if supplemental state standards are allowed to continue, we would urge Congress to direct HHS to first publish in the Federal Register its determination of which existing state laws and regulations would not be preempted by the federal rules before employers and others would have to comply with any state standards. It is simply unreasonable to expect every company and organization subject to these rules to take on this expense and burden and it is the only way to achieve any level of consistency and certainty under the current preemption standard. We also believe it should be the Department's continuing responsibility—not the public's—to review future amendments and additions to state laws and publish a notice after they have determined the effect, if any, of the new state requirement relative to the federal rules. Finally, there should be a clear safe harbor from enforcement actions or penalties if organizations are either in compliance with the federal regulations or are making good faith efforts to comply with a new state requirement until a federal determination is made.

The Department could carry out its responsibilities to review existing and future State privacy laws in a number of ways. For example, HHS could contract directly with legal experts who are familiar with state privacy laws or the Department could form a public advisory group to provide on-going review and advice on state standards as this field of law continues to evolve. Whatever course the Department might choose, it would be important the Department's findings on State laws be published in the Federal Register on a predictable basis, perhaps annually, and organizations be given a reasonable period of time to comply with the new requirements.

We also have significant concerns that the lack of a nationally uniform privacy scheme means that employers and others will face the prospect of uncertain enforcement actions and unpredictable financial damage awards under individual state laws. Even without a direct or implied right to bring a lawsuit under the federal rules, individuals could still bring lawsuits under individual state laws, as the discussion in the preamble of the regulation makes clear. The inevitable result will be increased litigation—or at the very least the increased risk of litigation—adding to health care premiums and leading to more contentious relationships with the many business partners that employers rely on to help administer the health plan choices offered to their employees.

Employers should have a single, uniform framework where the penalties for compliance failures are clearly understood and where appropriate limits are placed on amounts that may be recovered. The civil and criminal penalties in HIPAA would unquestionably serve as a meaningful deterrent for violations of

the privacy provisions. In our view, the Secretary of HHS should also be asked to examine the appropriateness of establishing a nationally uniform basis penalty scheme rather than exposing regulated entities to penalties under both federal and state laws.

THE CONSENT AND AUTHORIZATION PROCESS

The final privacy rules contain entirely new consent and authorization procedures that were not anticipated or proposed by HHS in the public comment stage for these regulations and could result in harm to individuals needing health care services. During the proposed rule stage, the Department had adopted the concept that prior individual approval was not necessary—and, indeed, was not permitted—as long as the information was used for certain specified purposes such as payment, treatment and health care operations. In the final rule, the Department retreated from its original position and has now required health care providers to obtain individual consent forms when a patient first seeks health care services.

We believe the required public comment process was circumvented by the entirely new and significant requirements added at the final rule stage. As a result, those who will be affected by the consent process standards had no opportunity to provide their views on the new procedures before they were finalized or to suggest improvements that clearly are needed.

We believe the new consent process in the final rule is likely to create significant complications and confusion. For example, individuals must be notified that they have the right to request restrictions in how their protected health information is used or disclosed for the purposes of payment, treatment and health care operations. Before these intended restrictions would become effective, the regulations provide for covered entities to agree to the limitation.

However, this process for reaching agreement on restricted consent forms can itself cause operational problems since each individual case will require a determination to be made as to whether the restrictions would impede access to needed information.

The regulations also require that individually-identifiable information may not be used or disclosed by health care providers without first obtaining an individual consent form from each patient. This is the aspect of the regulation that could, in fact, lead to actual harm to individuals seeking health care. What will happen to individuals seeking medical care or services in those unavoidable instances where no consent form has been obtained? In the absence of a signed consent form, the timely provision of such services could be significantly impeded. The likely disruptive effect of the mandatory consent form is inevitable unless this provision is revised before the compliance date occurs.

Clearly, many of these concerns with the consent process might have been addressed if the new scheme developed by the Department had been subject to public scrutiny in the proposed rule stage. Unfortunately, the procedures contained in the final rules are not only more complicated than necessary, but may also cause harm to those they are intended to protect.

THE "MINIMUM NECESSARY" STANDARD

The final rules adopt an ambiguous standard that covered entities may not use or disclose more than the minimum amount of information necessary for a particular purpose. The "minimum necessary" standard also must be applied when requests for health information are made from other sources as well as for setting policies and procedures to limit the amount of information disclosed or requested "on a routine or recurring basis." The rules assume, however, that this standard can and will be applied on a "bright line" basis; i.e., that those who receive protected health information should be able to make clear determinations about their "minimally necessary" information needs.

The regulation does not define "minimum necessary" or provide specific guidance on how to determine what information is the minimum necessary for a particular purpose. Despite this ambiguity, the rule imposes a duty on regulated entities to audit all their operations to determine, in advance of the compliance date, what information is minimally required by particular types of employees who are performing different duties with different information needs and to establish information access policies appropriate in each case.

The lack of clarity of the "minimum necessary" standard poses an immediate problem since the determination of what is "minimally necessary" will vary for a very wide range of different situations and will be interpreted differently in each case. Those who are not familiar with the information needs of a health care plan for particular purposes, for example, could easily have a much more narrow view of what is minimally needed than those responsible for making proper decisions on claims or for coordinating needed medical services.

Health care providers are the only ones who are exempt from the minimum necessary standard and then only when health information is being used for treatment purposes. We would recommend a "rule of reason" standard be authorized by the

regulation in applying the minimum necessary standard outside of the areas of health care treatment. Specifically, we would recommend that the minimum necessary rule be based on a prudent professional's determination of the information needed to accomplish an intended purpose. The rule of reason standard should also eliminate the need for advance determinations of the specific information needs of different categories of employees and provide more flexibility in future determinations about what

information is needed to continue to perform critical payment and health care operations functions.

NEW OBLIGATIONS ON PLAN SPONSORS

For employers, the final rule imposes entirely new obligations on the sponsors of group health plans that are difficult to interpret and, in many cases, may not achieve their intended purpose. Protecting employees from inadvertent or unwarranted disclosure of protected health information to anyone not involved in the administration of a health benefit plan is challenging because some employees wear several hats within the same organization.

In the case of a self-insured employer sponsored plan, the final rules appear to reverse the normal relationship between a group health plan and a plan sponsor. For an employer sponsoring a self-insured health plan, the legal entity known as the "group health plan" may consist entirely of legal documents describing payment arrangements and other details. The plan is not a defined organization (like an insurance company or HMO) or even an identifiable group of employees. The regulation contains nine specific conditions that the "group health plan" must require the "plan sponsor" to meet to ensure that the sponsor meets its obligations under the federal privacy rules. Since the group health plan is a legal creation of the plan sponsor, the conditions called for in the regulations would not be between two different parties, but would amount to requiring an employer to enter into an agreement with itself. This requirement hardly seems necessary since the regulations already preclude the use or disclosure of protected health information by a group health plan other than for the purposes of payment, treatment or health care operations unless an individual provides specific authorization for a uses beyond these areas.

The regulations also call for "adequate separation" between the group health plan employees with access to health information and other employees of the plan sponsor with no similar needs for health information. This "firewall" concept between plan sponsors and their group health plans is simply not possible to achieve in many cases, as the discussion in the preamble of the regulation acknowledges. The problem is most acute for smaller employers, where any information provided to the plan sponsor may be given to an individual who wears many hats within the company, only one of which may be related to health benefits responsibilities. For all practical purposes, it may not be either possible or desirable in these situations to share personal health information in these cases without it also being released to individuals with broader duties.

Even for larger employers, the attempt to segregate the employer's group health plan from its role as the plan sponsor will pose challenges since the regulations require plan documents to be revised after new parameters for the permitted uses and disclosures of health information have been established. The more active the employer is in the management of any of the functions of its group health plan, the more extensive the revisions that would be necessary in its operations, documents and its policies and procedures.

CONCLUSION

Again, I want to thank you, Mr. Chairman and members of this Committee, for the opportunity today to share our views with you. We look forward to working with you and your colleagues in taking the next needed steps on the HHS health care information privacy regulations. We remain confident that sensible improvements can be made to this regulation and hope to be of continued assistance as you examine this issue further.

The CHAIRMAN. Mr. Houston.

Mr. HOUSTON. Thank you, Mr. Chairman.

I am pleased to testify today on behalf of AHA's membership of nearly 5,000 hospitals, health systems, networks, and other providers of care.

UPMC, which is affiliated with the University of Pittsburgh School of Health Sciences, serves 29 counties in Western Pennsylvania and is one of the largest not-for-profit integrated health care delivery systems in the United States. We employ more than 25,000 people, and we are comprised of 16 owned and 10 affiliated hospitals. UPMC is also the leader in the development and use of electronic health care technology and systems.

I believe that I bring a significant amount of practical hospital operations experience here today.

I would like to make it clear that AHA has long supported the development of uniform national privacy standards. The need for such standards has become more pressing in recent years as information is increasingly shared electronically and as the delivery of health care has become increasingly integrated.

We appreciate this opportunity to present our views on HHS' final medical privacy rule.

Recently, the AHA sent a letter to Secretary Thompson, asking him to reopen the final rule implementing HIPAA's privacy requirements. We did so not because America's hospitals are recalcitrant on privacy, but because we believe that a better privacy rule would benefit patients and providers alike.

HHS' final rule on privacy will have a major impact on the day-to-day functioning of our Nation's hospitals. Providers will be required to make sweeping changes throughout their organizations and invest substantial resources in order to comply with this complex and pervasive regulatory scheme.

At UPMC, there are a variety of things that we believe we will have to do. We will be required to create entirely new departments to coordinate consents, authorizations, disclosures, and to evaluate and coordinate the requested changes to a patient's medical records.

We will need to make significant changes to policies, procedures, and processes, many of which will impose significant new requirements on staff who directly deliver care.

We will need to staff a HIPAA compliance office.

We will need to develop new information systems to track holistically consent authorizations and disclosures.

We are going to need to be able to modify many existing information systems, and in the case of the health system, we probably have on the order of 250 separate systems that we use to deliver care. We will need to modify them to ensure that access and disclosures are appropriate and to track all of the amendments and corrections and notations that might be requested.

We will need to evaluate and reopen many of our business contracts.

I agree that in all cases, we do put confidentiality provisions within our agreements, but each one needs to be scrutinized, and each one needs to be looked at in terms of the nature of the information that needs to be disclosed and the purpose of the vendor's need for information.

As you can imagine, this represents a significant amount of investment of time and resources, and this is time and resources that, frankly, I believe can be better spent on direct patient care.

HHS estimated that the 10-year cost would be about \$17.6 billion, and that is for hospitals, insurers, clearing houses and pharmacies. I can tell you that I believe, and based upon our own internal estimates in the AHA, this figure seriously underestimates the cost of implementing and complying with the privacy rule.

An AHA-commissioned study, for example, looked at hospital costs alone and found that the costs of only three key provisions in the proposed rule could be as much as \$22.5 billion over 5 years. Although some changes were made in the final rule that slightly reduced the cost, the fact is that the new rule will be exceedingly costly for hospitals and, as was stated earlier, many of these hospitals are struggling financially.

In this regard, the privacy rule represents yet another unfunded Federal mandate that hospitals must absorb. Because of the fact that 50 percent of hospital patients today are Medicaid and Medicare beneficiaries, we believe that Congress should closely examine the high cost associated with implementing the privacy rule and supply the necessary funds to ensure that the implementation does not put hospitals in financial jeopardy.

While the AHA strongly supports workable Federal medical privacy laws, we cannot support yet another unfunded mandate. The overwhelming financial impact of the final privacy rule is exacerbated by its overly aggressive implementation schedule. Hospitals are expected to be in full compliance with the new privacy rule by February 26, 2003. Adherence to that compliance schedule will be unattainable for many hospitals given not only the extensive operational changes that the rule will require changes to, but also the high cost associated with compliance.

I believe that the adoption of a more reasonable implementation schedule is essential.

Many important provisions contained in the final rule are either completely new or dramatically different from what was in the proposed rule. In some cases, those changes were welcome, such as relief from restrictions on sharing information with other caregivers outside the hospital; however, other aspects of the new rule, including potentially confusing and burdensome consent requirements and the inclusion of nonelectronic information and/or communications make compliance more complicated and problematic.

It is essential to fix requirements in the privacy rule that could impede patient care or disrupt essential hospital operations. For these reasons, Congress should encourage HHS to reopen portions of the privacy rule for comment.

Congress should also act to establish HIPAA as the national standard for protecting medical privacy by preempting State law. Lack of preemption of State law sets a carrying standard that can be problematic, especially for health systems that provide services in multiple States.

In conclusion, Mr. Chairman, America's health systems take very seriously the privacy of our patients' personal health information. We have a longstanding commitment to safeguard this privacy. But we also have a commitment to deliver high-quality health care to our patients.

The AHA looks forward to working with you to ensure that Federal standards for protecting patient privacy are appropriate and

workable. Additionally, UPMC invites this committee to Western Pennsylvania to see first-hand not only our information technology division, but to educate you on health care operations. We also offer to act as a model to determine what is truly workable.

Thank you.

[The prepared statement of Mr. Houston follows:]

STATEMENT OF THE AMERICAN HOSPITAL ASSOCIATION

Mr. Chairman, I am John Houston, information systems division director, data security officer, and assistant counsel for the UPMC Health System (UPMC). I am pleased to testify today on behalf of the American Hospital Association's (AHA) membership of nearly 5,000 hospitals, health systems, networks and other providers of care.

UPMC, which is affiliated with the University of Pittsburgh Schools of the Health Sciences, serves 29 western Pennsylvania counties and is one of the largest not-for-profit integrated health care systems in the United States. UPMC employs more than 25,000 people and is the largest non-governmental employer in the region. UPMC is comprised of 16 owned and 10 affiliated hospitals, as well as a managed care insurance company that serves more than 250,000 members. UPMC also operates over two dozen surgery centers and satellites, more than 300 physicians' offices, 10 long-term care and independent-living facilities, in-home services, a mail-order pharmacy, a regional reference laboratory, rehabilitation and occupational medicine services, and international health care initiatives.

BACKGROUND

The AHA has long supported the development of uniform national privacy rules. The need for national standards has become more pressing in recent years as information is increasingly shared electronically, and as the delivery of health care has become increasingly integrated. We appreciate this opportunity to present our views on the final medical information privacy rules issued by the Department of Health and Human Services (HHS) on December 28, 2000 that implement provisions of the Health Insurance Portability and Accountability Act (HIPAA).

THE PROBLEMS WITH HIPAA AND WHAT CONGRESS CAN DO

On January 31st, the AHA sent a letter to HHS Secretary Thompson asking him to re-open the final rule implementing HIPAA privacy requirements. We did so, not because America's hospitals are recalcitrant on privacy, but because we believe a better privacy rule would benefit patients and providers alike.

HHS' final rule on medical records privacy will have a major impact on the day-to-day functioning of our nation's hospitals. Providers will be required to make significant changes throughout their organizations and invest substantial resources in order to comply with this complex and pervasive regulatory scheme. Because nearly 50 percent of hospitals' patients are Medicare and Medicaid beneficiaries, we believe Congress should closely examine the high costs associated with implementing the privacy regulation and take the necessary steps to ensure that implementation does not put hospitals in financial jeopardy by supplying the necessary funds. While the AHA strongly supports workable federal medical privacy laws, we cannot support yet another unfunded mandate.

The overwhelming financial impact of the final privacy rule is exacerbated by its overly aggressive implementation schedule. Hospitals are expected to be in full compliance with the new privacy rule by February 26, 2003—just a little over two years from now. Adherence to that compliance schedule will be unattainable for many hospitals given the extensive changes in overall operations the new privacy rule will require and its high cost. Adoption of a more reasonable implementation schedule is essential.

Many important provisions contained in the final rule were either completely new or dramatically different from what was in the proposed rule. In some cases, those changes were welcome, such as relief from restrictions on sharing information with other caregivers. However, other aspects of the new rule, including potentially confusing and burdensome consent requirements, raise serious concerns. It is essential to fix requirements in the privacy rule that could impede patient care or disrupt essential hospital operations, and to that end, Congress should encourage HHS to re-open portions of the new privacy rule for comment.

Congress should also act to establish HIPAA as the national standard for protecting medical privacy by preempting state law. Lack of preemption will create huge

and unnecessary burdens for providers without providing patients with significant additional safeguards for their medical information.

HHS' FINAL PRIVACY REGULATIONS

The final privacy rules issued by HHS addressed some of the concerns raised by America's hospitals. Most importantly, the "minimum necessary" standard now exempts disclosures by providers in one hospital to providers in another hospital for treatment activities. That means physicians and nurses will more likely have access to the patient information they need to treat patients, particularly in emergency situations. In addition, the final rule no longer requires that hospitals directly monitor the business practices of every business associate. Finally, hospitals are allowed to use patient information for fund raising purposes as long as fund raising is listed in a hospital's notice of privacy practices and patients are permitted to opt out of receiving those solicitations.

While we are pleased with these changes, several aspects of the regulation cause significant concern, which is why we asked Secretary Thompson to re-open them.

THE REGULATION'S COST

The HHS rule requires significant and costly changes to hospitals' current information systems, and in many cases will require that hospitals build or acquire expensive new information technology solely to meet HIPAA requirements, including tracking disclosures of information. The new rule will also require hospitals to hire additional staff, institute additional staff training programs, re-open contracts with every business associate (which can number as many as 5,000 for an integrated health system), and spend significant resources trying to determine whether they must comply with conflicting state laws and, if so, revamping their compliance efforts. Such sweeping changes are enormously costly and conflict with HIPAA's explicit cost-reduction goals.

For hospitals, the effort and cost of compliance will be significant. This is because patient medical information is typically stored in a variety of mediums and at many locations. In the absence of an enterprise-wide electronic health information environment, the tracking and coordination of patient medical information for the purpose of compliance will be difficult. While UPMC is implementing such a state-of-the-art health information environment, it is a time-consuming and extremely costly undertaking. Most health care providers simply do not have this capability, nor the funds necessary to achieve it. In the alternative, should UPMC choose to comply through individual compliance plans at each facility, UPMC will be unable to fully integrate operations, which is necessary to make substantive advancements in patient care and maximize efficiency.

HHS itself estimated the regulation to have a 10-year cost of \$17.6 billion for the entire field, including hospitals, insurers, clearing houses and pharmacies. The department's final estimate considered all of the rule's provisions except preemption of state law. HHS claims that the costs of complying with the privacy regulation will be offset over the course of a decade by savings accrued as a result of HIPAA's transactions standards.

We believe that HHS has seriously underestimated the costs of implementing and complying with this privacy rule. An AHA-commissioned study, looking at hospital costs alone, found that the cost of only three key provisions of the proposed rule (minimum necessary, business partners and state law preemption) could be as much as \$22.5 billion over five years. This estimate depended on whether hospitals could comply by simply modifying existing information systems, or if replacement or significant reconfiguration of those systems was required. Although some changes were made in the final rule that may slightly reduce the cost, the fact is that the new rule will still be exceedingly costly for hospitals, many of which are struggling financially. In this regard, the privacy rule represents yet another unfunded federal mandate that hospitals must absorb.

ADMINISTRATIVE REQUIREMENTS

The final rule is lengthy and prescriptive. HHS specifically requires hospitals to provide patients with notice of a hospital's privacy practices, and to obtain their consent or authorizations. For example, the rule specifies: how patients receive notice of their rights; how providers obtain consent from their patients; and when separate authorizations from patients are needed and the procedures for documenting such authorizations.

The final rule also imposes a myriad of new administrative duties. For example, hospitals must: designate a privacy officer who is responsible for developing and implementing privacy policies and procedures; provide a process by which patients

may inspect, copy and amend their medical records, and receive an accounting of disclosures of their medical records; and re-open contracts with business associates, including attorneys, auditors, vendors, suppliers and consultants, to include the hospital's privacy practices with which each business associate must comply.

What do these requirements mean for hospitals? For UPMC, we expect that we will have to: Create entirely new departments to coordinate consents, authorizations and disclosures and to evaluate and coordinate requested changes to patients' medical records; Make significant changes to policies, procedures and processes—many that will impose significant new requirements on staff who directly deliver care; Staff a HIPAA compliance office; Develop significant new information systems to track consents, authorizations and disclosures; Modify existing information systems to ensure that access and disclosures are appropriate; and Evaluate and re-open business contracts.

In order to comply with HHS' privacy rule, UPMC will have to make a significant investment of time and resources' time and resources that we would prefer to spend on direct patient care, not paperwork.

PREEMPTION OF STATE LAW

Hospitals and health systems consider themselves guardians of our patients' individually identifiable health information. That is why the AHA has long supported the passage of strong federal legislation to establish uniform national standards for all who use this information.

Unfortunately the final rule provides a floor rather than a ceiling for preemption of state law. Any state law that is contrary to and more stringent than the federal standard is not preempted. This will require hospitals to determine what the laws are in each and every state in which they do business and then make an educated guess about which apply.

One of our primary reasons for supporting federal confidentiality legislation is that health care is delivered across state boundaries. National uniform rules are needed to establish a strong uniform privacy protection across the country. Matching up many different state rules is increasingly difficult, and will lead to frustration and confusion without, in all likelihood, providing any appreciable additional privacy protection for patients.

At the very least, HHS should analyze which state laws preempt HIPAA and do so promptly before hospitals begin to make changes to their systems based on HIPAA's mandates. However, the real solution to this dilemma is for Congress to act to preempt state laws altogether. HIPAA provides a comprehensive framework to assure a more than adequate protection for patients' medical information. Allowing state laws to preempt HIPAA is unnecessary for both patients and providers.

RELEASE OF INFORMATION TO LAW ENFORCEMENT

We remain concerned that the standards under HIPAA are too lax with respect to law enforcement authorities. It is ironic that a regulation establishing a myriad of new checks and balances on the use and disclosure of confidential medical information makes it too easy for law enforcement authorities to obtain that information and potentially misuse it.

New Provisions to the Final Rule

In a departure from the proposed rule, HHS introduced a provision on patient consent, which is required when protected health information is used or disclosed for purposes of treatment, payment or health care operations. Patient consent forms must be separate from privacy notices, signed by the patient and retained by the hospital. If a patient subsequently revokes his/her consent, hospitals must discontinue using the protected health information and advise business associates to do the same.

Our concern about this consent process is that it was not subject to meaningful notice and comment. Neither the AHA, nor other affected providers, had an opportunity to comment on how this potentially confusing and burdensome procedure would affect patient care or hospital operations. Therefore, it is only prudent to re-open the rule so that the pros and cons of HHS' imposed consent scheme can be fully considered.

HHS also expanded the definition of protected health information to include all health information, not just electronic but also written and oral communications. HHS' decision to cover "oral communication" is perplexing and potentially troublesome and one of the areas mostly clearly beyond the authority given to the former HHS Secretary by Congress.

Our concern about having HIPAA cover "oral communications" is that it can lead to unintended and certainly unfortunate results. For example, if a patient is sharing

a room with another patient, which is often the case, physicians may be constrained to discuss openly vital care and treatment issues for fear of running afoul of HIPAA's many prohibitions on use, disclosure or tracking of patient medical information.

CONCLUSION

Mr. Chairman, America's hospitals and health systems take very seriously the privacy of our patients' personal health information. We have a long-standing commitment to safeguarding this privacy, but we also have a commitment to deliver high-quality health care our patients need. The AHA looks forward to working with you to ensure that federal standards for protecting patient privacy are appropriate and workable.

The CHAIRMAN. Thank you, and I thank you all for excellent statements.

I will now question you a little bit, and we will reserve the right to ask additional questions after the panel has concluded.

Ms. Goldman, law enforcement agencies may access medical records only after a legal process that includes a warrant, court order, or administrative subpoena. Please elaborate on your specific concerns regarding access to medical records by law enforcement agencies. What additional access requirements would you recommend, if any?

Ms. GOLDMAN. We believe that under the regulation, law enforcement should not be able to get access. In other words, health care providers and plans should not be able to disclose to law enforcement unless there is legal process, which is what the regulation requires.

However, where the regulation stops short is that it allows for legal process such as a civil investigative demand that does not have to get approval by a neutral magistrate, does not have to go through a judge, but could be issued just from a supervisor in that office. So we think that it will not fairly balance the privacy issues and the law enforcement issues the way we usually do in a Fourth Amendment context. That is where we are looking to see something strengthened.

But honestly, the law enforcement section in there is certainly a vast improvement over what we have today, where there is no legal requirement of any kind of process.

The CHAIRMAN. Ms. Greenman, you mentioned the final rule's treatment of group health plans and plan sponsors as an attempt to create fire walls that would protect an employee's health information from being used for employment purposes. Does it make sense that the group health plan has the authority to withhold information from the plan sponsor, since that is where the plan gets the information in the first place?

Ms. GREENMAN. Bear in mind, Mr. Chairman, that many large employers in particular have self-insured plans where the plan is not a separate legal entity but merely a paper document. So that while we completely support the notion that there should be absolutely no improper use of medical information or health-related information that could facilitate discrimination in hiring, firing, promotion, and that health information should not be part of personnel records, there are situations in which a complete fire wall is impossible, because you have one person wearing multiple hats.

Another area where concerns arise has to do with the legitimate implementation of rules to effectuate the Americans with Disabil-

ities Act, reasonable accommodation, Family and Medical Leave Act provisions, and the like, and without some interaction between, say, a supervisor who needs to work on how can a job be modified in order to accommodate the specific disability requirements of an individual, if there is a complete fire wall and no opportunity for dialogue, I think we have a problem.

The CHAIRMAN. Thank you.

Mr. Houston, one of the major themes of today's testimony is that there is not sufficient time to implement the final regulation. What time frame would be more reasonable in your judgment?

Mr. Houston, I think there are a couple of ways to look at this. I think there are certain provisions that I believe can be implemented within the 2-year time frame, so I believe that we should be trying to work toward compliance on certain provisions within 2 years. Yet, being an information systems professional and someone who works with computers and health care applications on a daily basis, I also feel very strongly that it is going to take more than 2 years to modify all the different systems that we use.

It is going to take a long time to understand exactly what we need to do, and frankly, because of budget pressures, we need to put a plan together that both reasonably allows us to modify those systems and add new systems while also being done in a time frame that we can, frankly, from a financial perspective absorb or that is palatable to us. So I think that a more reasonable time period is at least 1 year, possibly two. But again, there are certain pieces that we should be doing within a 2-year time period or that we can, reasonably.

The CHAIRMAN. Thank you.

Senator Dcdd.

Senator DODD. Thank you very much, Mr. Chairman, and let me thank our witnesses.

Let me also say to the next panel that I want to apologize in advance for not being able to be here for their testimony, but I appreciate it very much. In fact, I had a chance to meet with Mr. Heird from Blue Cross/Blue Shield before the hearing, Mr. Chairman, and heard some of their issues, and Judith Lichtman and I talk often, so I am very familiar with her interest in this subject matter as well.

I thank the chairman for holding the hearing. This is the first hearing that we have had on the subject matter in this Congress. In fact, I am leaving here to conduct a press conference with Senator Shelby. He and I have put forward legislation dealing with the use of children in surveys in schools, where some marketing companies are actually going into classrooms and doing surveys on kids on subject matter like what cereals they like, I might add. There is some concern about parental consent and school consent for this kind of activity, which is a related matter in terms of privacy and permission, opting in and opting out.

Let me just make a couple of observations, and then I have a question for you, Ms. Goldman. First of all, this is not a new issue. Concerns about our privacy have been around for a while, and it is beginning to sound like this is some new discovery that we have come across. I admitted earlier that I conducted a survey about 8 years ago and discovered that my constituents were deeply inter-

ested—I did not create the interest in it; they had the interest. Trying to protect people's privacy in a variety of areas has always been a matter of deep concern, and clearly in the medical field, this is not a newfound issue for people.

I am sensitive to the time question about implementation. Mr. Heird mentioned this to me, and we talked about it. I think that all of us here want to have this done right. We realize that with a lot of the technology questions, the mergers and so forth that are occurring, the time needed to get this done properly is certainly a legitimate issue. But I would hope that we will not get into the issue of reopening. It seems to me that there are plenty of ways in which we can modify or do things, but reopening this process I am deeply worried about, Mr. Chairman. I know what that means. It is not terribly subtle in terms of what this does.

I will tell you that the public cares about this very, very much, and any indication that we are backing up on this thing, we will be faced with some laws passing on the floor—I will tell you right now that if you bring up a privacy bill on the floor of the U.S. Senate, and it is worded anywhere near cleverly, it is going to pass; it is going to pass. There are unintended consequences of legislation that may be crafted rather quickly, but it is a very potent issue, so I would strongly urge HHS—and I presume they are listening today—to go back and review if you want to, but reopening the regulations is something that I would be very reluctant to see occur.

So let me ask you about that, Ms. Goldman. We have heard from groups and from both of our witnesses here. What would be the effect of reopening the regulations, in your view?

Ms. GOLDMAN. Senator, I appreciate your remarks and also appreciate your suggestion that if a privacy bill were to come to the floor, it would pass, because we do need to look at ways to strengthen and improve on the regulation through legislation.

We believe that in the memorandum that was circulated by Chief of Staff Card that talked about the moratorium on regulations, there is an explicit exception for regulations mandated by statute, and we believe that this fits within that.

In addition, the regulation is about to become effective, and after that occurs, there are opportunities for Secretary Thompson to modify the regulation where it is necessary, as the regulation says, to permit compliance.

Some of the letters that you have seen that have gone to the Secretary asking for a delay give certain examples of things that might not occur if the regulation goes into effect. Our lawyers think that those are not accurate examples, that there has been a lot of misinformation out there about the impact of the regulation.

I think it would be more prudent to move forward and to look at specific instances on a case-by-case basis of where there might be hurdles to implementation, where there might be problems with compliance.

We all want to make sure that the regulation works. No one is trying to keep information from flowing to treat people, to pay for their care, to conduct outcomes analyses, to do research in this country. We care very much about that, and many of our groups—

the Consumer Coalition and provider groups that we work with—care very much about this as well.

So I would suggest that we sit down and look at specific issues that might be hurdles to compliance and really try to sort through whether those are accurate, whether they may be overblown, whether there could be guidance issued from the administration to calm some of the fears that are out there.

But right now, we believe that the regulations should go forward and should not be delayed.

Senator DODD. Let me also ask you about the time issue. What is your view on the time question? Actually, it would be 3 years from the time of enactment, but 2 years here before these regulations would come into force. Are you wedded to that? If there were some argument made for an extension of 6 months, a year, a year and a half, whatever it may be, how would you feel about that?

Ms. GOLDMAN. Well, Senator, I appreciate the comment that you made that this is not a new issue. Many of the provisions in the regulation should be very familiar to the groups that are going to have to comply with this.

The groups that I think have a real hurdle are the safety net providers, the community clinics, those that do not have the resources to hire lawyers to tell them how to comply and what is the best way to comply. We are looking to do some implementation guidance for them. They are the ones who are really going to need the help.

But the way that the regulation is drafted, it allows for the implementation to be scaleable so that those smaller entities can do what makes sense for them and do what is appropriate in that context. We would not support any delay in implementation of the regulation. We believe that the regulation has to be implemented hand-in-hand with the transaction standards, which will absolutely save money over time, and that they need to be implemented together. Otherwise, you are looking at a redesign two times; you are looking at the transaction standards being put into place, and then, later on down the road, trying to build privacy protections into those systems, and you are going to hear a cry from many of these same groups that "We cannot do it; we have to do a whole new redesign."

So I would oppose any delay in implementation and would hope that as we go forward, groups can come forward and say, "We are having trouble with compliance. Here are some of the hurdles that we are having," and we can sit down and look at them. But to have an initial reaction to not wanting to be regulated in this context and asking for a delay, I think is not the way to go.

Senator DODD. I thank you for that.

Mr. Chairman, as you know, I have joined the Caucus on Privacy, which is a bicameral caucus headed up by Senator Shelby in the Senate, Joe Barton, a Republican House Member, and Ed Markey of Massachusetts and myself, on a wide range of issues, and as I said, there are not only bicameral but bipartisan concerns on a wide range of privacy issues, but this is one of the primary ones. So I would again urge the interested parties here that this is time to go to work on this and get it done right. Fooling around with reopening the regulatory process here is going to provoke addi-

tional legislative efforts to insist upon this, and that could even compound the matter worse. So I would urge those who are advocating reopening to rethink the position and just try to get to work and see if we cannot get this done right.

Mr. Chairman, I thank you for your time and thank the witnesses, and I apologize again to the final panel.

The CHAIRMAN. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Chairman, we face a dilemma. There is no doubt in my mind—and I agree with Senator Dodd's comments in this regard—that patients are very concerned and apprehensive about the confidentiality of their medical records. Furthermore, it seems evident to me that the patchwork of laws that we have now which attempt to safeguard those records is inadequate.

I also recall our efforts last year to try to come up with a medical privacy bill, and that we did not succeed in doing so because this is such a complex and difficult challenge.

There is also, however, no doubt in my mind that the regulations proposed by HHS are extremely burdensome, complex, and costly for many health care providers.

I am also concerned, based on a meeting I had this week with two physicians' assistants from the State of Maine, that they could create practical problems that would impede the smooth delivery of care to patients. So that clearly, the goal of protecting records and ensuring confidentiality is one that we can all embrace, but its practical implementation turns out to be very difficult.

I do want to ask the panel to comment on an issue that everyone has raised, and that is the cost of the regulations. It is my understanding that HHS has estimated that the cost to comply with the regulations would be \$17.6 billion over the next 10 years. However, HHS also estimated that as a result of administrative simplification standards included in the regulations, there would be savings of nearly \$30 billion over that same 10-year period. That obviously, if HHS is correct, would more than offset the cost of compliance and would indeed produce net savings in excess of \$12 billion.

I would like to have each of you comment on your assessment of the validity of those statistics.

Mr. Houston, we will start with you.

Mr. HOUSTON. Let me comment, because that is an area where I probably have the most knowledge here. An organization the size of the UPMC health system already does an enormous amount of electronic transactions. That is primarily how we bill. So if there is an assumption that we are going to become more efficient by doing standardized electronic transactions, I would say no, because we already do electronic transactions; to go back and reformat them into a standard costs us money, and frankly, the return is not there.

So I do not believe that we are going to net out the savings in comparison to all the costs that we are going to incur.

One thing that we have not spoken about here, as we are primarily talking about privacy, is that there is also a companion piece of HIPAA regarding security. I look at both of those as being almost inseparable. They do speak to different things, but when you are trying to solve the problem, you have got to address both.

I believe that for the health system, we are going to spend between \$40 and \$50 million to deal with both of those issues—at least. That is an enormous amount of money. A lot of health systems do not have that kind of money to invest today. So even if you are going to get returns later, and even if they do not do electronic transactions later, they may not be able to spend the money up front.

I think there are real issues about how you pay for it, when you get returns, if you get returns.

Senator COLLINS. Ms. Greenman.

Ms. GREENMAN. While I cannot comment on the specific dollar amounts, I would say that the pluses and minuses do not match, because the pluses, even if they were real, may be realized by different entities than those entities that would have to incur significant additional cost.

For example, for employers, you can click off right off the bat some of the additional expenses—you need a privacy officer, you need privacy policies, you need implementation, you need education, you need to enter into new contracts with all of your business partners and health plan providers, administrative service providers. You need to modify all the systems. And I will tell you as someone who has witnessed the complexity of making even minor changes in benefit programs that the amount of time and expense that goes into what appear to be minor changes is astonishing. The legal fees to figure out what constitutes compliance, to work through the maze of these different rules and to, at the end of the day, really just have a guess as to whether, after all of this, you are in compliance or you are not in compliance, the cost will be tremendous, and I think there is a much simpler way to get there.

Senator COLLINS. Ms. Goldman.

Ms. GOLDMAN. Thank you, Senator.

I can only take the numbers that were produced at face value; I am not in a position to evaluate them. However, what I do know is that 5 years ago when I was working with a number of industry groups on the administrative simplification language which is now in HIPAA, there was a tremendous push and a desire to see the transaction standards go forward because there would be ultimate cost savings. There were many in the health care industry who very much wanted those transaction standards in place, so it would be easier and cheaper and more efficient and more beneficial to share information across various health care entities.

The way the privacy language got in there was because there was such fear that other groups, consumer groups, had that if we moved forward with the transaction standard, we would create an electronic health information network without any privacy protections in place, and that was seen as untenable.

So the reason that they are linked is because yes, there will be cost savings and there is a benefit, but we will never see that benefit unless we protect privacy.

So I would say to you that even if we found that there were some costs associated with implementing the privacy rule—and I believe, as you have said, that there will be—that it is the right thing to

do and that many responsible health care entities right now should be doing it today—they should be doing it now.

Senator COLLINS. I see that my time has expired.

The CHAIRMAN. Please go ahead.

Senator COLLINS. Thank you. I do want to just raise very quickly one other issue.

I notice, Mr. Houston, in your written statement that you raise concerns about the easier access that law enforcement would have to medical records, and I remember bringing up this issue with Secretary Shalala when the proposed regulations first came out, and I believe, if memory serves me correctly, that it was easier for law enforcement officials to gain access to confidential medical records than to videotape rental records.

Is that still true in the final regulations? Is there still more work to be done in that area?

Ms. Goldman, do you want to start?

Mr. HOUSTON. I can speak to that, and I think I am going to mirror a lot of what Ms. Goldman had also stated.

Ms. GOLDMAN. Go ahead.

Senator COLLINS. All right.

Mr. HOUSTON. I think, though, that the regulations can go somewhat farther. There are concerns that law enforcement at times, even with some type of oversight, still has carte blanche to make these wide forays into the medical records, to go searching for things or whatever.

I think that what we are asking for is additional protections so that that does not occur. Law enforcement where necessary needs to have access to such information. We just want to make sure that it is appropriate, reasonable, and it gives us assurances that there is some process in place that, when they ask for information, it is necessary for what they need to do with it.

Senator COLLINS. Thank you, Mr. Chairman.

The CHAIRMAN. I want to thank the panel. We have to go to the next panel now, but I can assure you that we will probably be back to you with additional questions and use you as a resource during the period of the next couple of years or even next week.

Thank you very much for your testimony. We look forward to working with you.

I am very pleased to introduce our third and final panel of witnesses, including a patient advocate, a researcher, and a representative of the managed care insurance industry.

First, I would like to welcome Ms. Judith L. Lichtman, president of the National Partnership of Women and Families of Washington, DC. Under her leadership, the National Partnership has worked to advocate every important piece of legislation concerning women and families over the past 25 years. She is a graduate of the University of Wisconsin Law School, and her professional credits include positions at The Urban Coalition and the U.S. Commission on Civil Rights, and as legal advisor of the Commonwealth of Puerto Rico. She has received the Leadership Conference on Civil Rights Hubert H. Humphrey Award for her contributions to the advancement of human and civil rights.

Ms. Lichtman, welcome. It is a pleasure to have you here this morning. Please proceed with your statement.

STATEMENTS OF JUDITH L. LICHTMAN, PRESIDENT, THE NATIONAL PARTNERSHIP FOR WOMEN AND FAMILIES, WASHINGTON, DC; DR. G. RICHARD SMITH, JR., DIRECTOR, CENTERS FOR MENTAL HEALTHCARE RESEARCH, UNIVERSITY OF ARKANSAS FOR MEDICAL SCIENCES, LITTLE ROCK, AR, ON BEHALF OF THE ASSOCIATION OF AMERICAN MEDICAL COLLEGES; AND ROBERT C. HEIRD, SENIOR VICE PRESIDENT, ANTHEM BLUE CROSS AND BLUE SHIELD, INDIANAPOLIS, IN, ON BEHALF OF BLUE CROSS/BLE SHIELD ASSOCIATION

Ms. LICHTMAN. Thank you, Mr. Chairman.

As you noted, I am here today representing the National Partnership for Women and Families, and I am grateful to you and to Senator Kennedy for having invited me.

I respectfully request that our full statement be included in the record, and I will stick to my 5 minutes.

The CHAIRMAN. Thank you. That will certainly be done.

Ms. LICHTMAN. The National Partnership is a national advocacy organization dedicated to improving the lives of women and families. Improving access to high-quality health care is, of course, an integral part of that mission, and privacy of medical information is an essential component of high-quality care.

Many if not all of the Senators indicated in their questions this morning your recognition that there is a deep and profound fear on the part of patients that they have lost control over their private medical information. And women, I would suggest to you, are probably more worried and, in the vernacular, more scared than one can imagine.

As recently as the week before last, in focus groups that we were doing around the country asking women about the ways in which they could be helped in accessing their own health plans, they inevitably wanted to turn the conversation to privacy—a subject about which we had no intention of asking questions.

I tell you that tale to show you the intensity of the feeling out there. We were asking questions about “X” and they wanted to talk about privacy.

The fear is so profound that women will withhold information because they are afraid of how the information is going to be used. And the converse or the flip side of the coin is as well true—they will fail to ask for information in fear that just asking for information will divulge questions about their personal health status that they do not want to share.

Women are especially nervous about their employers knowing too much about them, and they are very worried that those employers are going to find out about their health or medical conditions.

We have an obligation to make sure that that health information is kept confidential. Without that insurance, the very quality of care that individuals receive is compromised.

We applaud HHS for promulgating this final regulation. We think it is a huge breakthrough for people, and finally, we have the Federal Government taking the necessary steps to promote the kind of confidence in privacy of medical information that will go a long way toward improving that quality of care.

On the whole, the regulation strikes exactly the right balance between protecting privacy on the one hand and respecting legitimate uses and disclosures by covered entities, and it does so, as Senator Collins just noted, in a very complicated world.

Let me focus on why this regulation is so very critical to women. The regulation goes about as far as it can to protect women from inappropriate disclosures to employers and from inappropriate uses by employers. The only reason the regulation cannot do more is perfectly obvious—it is constrained by HIPAA. By enacting a law that directly reaches employers, Congress could alleviate lingering and legitimate concerns about misuse of information by employers, but it would clearly be up to Congress to do so.

The regulation protects the privacy of women seeking sensitive services by allowing them to request restrictions on how that information is used and where the information is sent. For instance, there would be no more phone messages or answering machine messages that can be heard by the entire household. The regulation provides special treatment for psychotherapy notes. Nearly all uses and disclosures for such notes require a very special authorization. It protects the privacy of young women and protects them from harm.

It respects the important role that parents generally play in obtaining health care for their children, but it also recognizes the need to let minors continue to control their own protected health information in particular and narrow circumstances.

It also protects victims of domestic violence from further abuse. It gives them the power to object to disclosures about them to law enforcement officials, as Senator Collins just noted, as getting law enforcement involved can often lead to further abuse by the abuser, and the regulations recognize that problem. If the police are given information without their agreement, the woman must get notice so she has a chance to protect herself from retaliation.

This privacy regulation is an important milestone, and HHS has done an excellent job of reconciling the diverse interests of the various stakeholders, and we hope that Congress will not upset this balance.

Any action by Congress should be to strengthen it and fill the HIPAA gaps, not to undermine it. HIPAA gaps include failure to cover all people who have access to medical information and failure to provide meaningful enforcement. Frankly, we prefer congressional inaction to congressional erosion of this regulation.

Because it is so important, we also urge Congress to ensure that HHS has the resources it will need to properly implement and enforce this regulation, even more important, since, as has been noted earlier, there is no private right of action, and individuals must rely on HHS to enforce this.

Thank you.

The CHAIRMAN. Thank you.

[The prepared statement of Ms. Lichtman follows:]

PREPARED STATEMENT OF JUDITH L. LICHTMAN

I am Judith Lichtman, President of the National Partnership for Women & Families. I would like to thank Chairman Jeffords and Senator Kennedy not only for the opportunity to testify today, but also for your leadership and longstanding commitment to a range of issues that are vitally important to women and families.

The National Partnership for Women & Families is a national advocacy organization based in Washington, D.C., and dedicated to improving the lives of women and families. Improving access to high quality health care is an integral part of our mission. Privacy of medical information is an essential component of high quality care. Medical privacy is especially important to women because they are the greatest users of health care services and because of their need for sensitive services like reproductive health and mental health services. Medical privacy is also especially important to women who are victims of domestic violence because inappropriate disclosures can threaten their personal safety and that of their children.

Women across America have a deep and profound fear that they have lost control over their private medical information. Without confidence that private information will remain just that—private—women are reluctant to share information with their health care professionals—to the detriment of their own health. Fear that medical information is not kept confidential also keeps women from obtaining health care services in the first place, or forces them to go outside their health plan and incur significant out-of-pocket expenses.

Strong and enforceable privacy protections are needed now more than ever thanks to the recent changes in our health care system. The rise of managed care means that more people have access to a person's medical information. The computer revolution makes immediate transfer and disclosure of such information possible, but also brings with it the possibility of strong safeguards against inappropriate use and disclosure.

We had hoped that Congress would meet its own self-imposed deadline of August 21, 1999, and enact comprehensive privacy legislation. Unfortunately, Congress failed to meet that deadline.

We applaud the Department of Health and Human Services (HHS) for stepping up to the plate and promulgating the final regulation that was published in the Federal Register on December 28, 2000. This regulation is an important breakthrough in the effort to protect the privacy of health information. Federal action in this area was long overdue. We believe this regulation will go a long way toward promoting confidence in the privacy of medical information and improving the quality of care.

Although we have concerns about some particular provisions, on the whole, we believe that the final regulation strikes the right balance between protecting privacy and respecting legitimate uses and disclosures by covered entities. We believe the regulation will allow the health care system to function efficiently and without significant impediment.

GAPS IN HIPAA

As a general matter, some of our major concerns with the regulation stem from flaws in the authorizing legislation, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), rather than from policy judgments entrusted to HHS. There are two primary gaps in privacy protection due to limitations in HIPAA. The first involves the reach of the final regulation, and the second involves the remedies of patients whose privacy rights under the regulation are violated.

First, the final regulation does not, and cannot, reach all of the people or entities that create or have access to medical information. It only covers most, but not all, health care providers; health plans; and health care clearing houses. As discussed more fully below, its failure to cover employers, even though it does cover health plans sponsored by employers, adds complexity to the regulation and puts people at risk for privacy breaches.

Second, the final regulation does not provide meaningful enough remedies for people when their privacy rights are violated. Enforcement will be largely through HHS. Patients whose rights are violated can file a complaint with the covered entity or with the Secretary of HHS, but the regulation does not create a private right of action for damages. We are concerned that covered entities will not have a strong enough incentive to comply with the regulation and that patients who are harmed by violations will go uncompensated.

Only Congress can fix these holes. We hope that Congress will enact legislation to fill in these holes, while at the same time not undermining the important protections incorporated into the regulation. Frankly, we would prefer congressional inaction to congressional erosion of the new important privacy rights in the final regulation.

GENERAL COMMENTS ON THE FINAL REGULATION

We are particularly pleased with two changes that HHS incorporated into the final regulation: (1) the extension of the regulation to health information regardless

of the form, including oral information; and (2) the addition of a consent requirement for health care providers.

The final regulation makes clear that it applies to all individually identifiable health information in any form, not just to information that had been maintained or transmitted electronically at some point. This will give patients a higher degree of protection for personal health information, make the privacy standards easier to implement and enforce, and further HIPAA's goal of encouraging a computer-based health information system.

We also applaud the inclusion of a consent requirement for uses and disclosures by covered health care providers. We disagreed with the approach in the proposed rule because it not only lacked a consent requirement, it generally prohibited providers from seeking patient consent. Patients should be encouraged to be active participants in their own health care—and the consent process should be an integral piece of that picture. We would have preferred that health plans also be required to seek an initial consent from the patient and were disappointed that the regulation did not include such a requirement.

We are extremely concerned about the new provisions in the final regulation concerning marketing and fund raising by covered entities. These provisions could very well result in an avalanche of marketing and fund raising appeals from third parties unknown to the individual. Although the fund raising provision limits the type of personal health information that can be used and disclosed for this purpose, the marketing provision contains no such limitation. Indeed, the marketers can target people precisely because they have a particular medical condition. There was no similar provision in the proposed rule. We believe that covered entities should not be allowed to use protected health information for these purposes absent explicit authorization from the individual. The after-the-fact opt-out provided in the final regulation is insufficient because, by definition, the information will already have been disclosed.

COMMENTS ON SPECIFIC ASPECTS OF THE FINAL REGULATION THAT ARE OF PARTICULAR IMPORTANCE TO WOMEN AND FAMILIES

The final regulation in its entirety provides important new protections for women and families, but the rest of our testimony will focus on aspects of the final regulation that are of particular importance to women and families. We address how the final rule deals with employer-sponsored health plans; critical protections for women (including young women) who seek sensitive services; the rights of minors; and important new protections for victims of domestic violence.

Role of employers that sponsor health plans

Most women and families get their health insurance through employer-sponsored health plans governed by ERISA (the Employee Retirement Income Security Act). Many fear that employers know more than they should about employees' (and dependents') private medical information and may use that information inappropriately to make employment decisions. The final regulation goes as far as it can to protect workers and their dependents from inappropriate disclosures to employers and from inappropriate uses by employers.

HIPAA and the final regulation reach most ERISA plans, though not the employer or other plan sponsor. The final regulation refers to the following ERISA plans as "group health plans" and includes a number of provisions for just these types or plans: ERISA plans that have 50 or more participants; and ERISA plans, regardless of size, that are administered by an entity other than the employer who established and maintains the plan.

The combined effect of the special provisions for these "group health plans" is that protected health information can be shared with the employer/plan sponsor only in limited circumstances and only when certain requirements are met. The regulation does this by reconciling the employer/plan sponsor's legitimate need for access to some information with the need to ensure that protected health information is not used for employment-related purposes or purposes unrelated to the management of the group health plan.

How these provisions work is best illustrated by the common situation in which an employer-sponsored group health plan contracts with a health insurance company or HMO to provide health benefits. In such a case, the employer/plan sponsor needs access to very little protected health information and only for limited purposes. Special provisions apply in cases where the employer/plan sponsor only needs "summary health information" for the purpose of soliciting bids from a new/potential insurer/HMO or for the purpose of modifying or amending the plan. (Summary health information is defined as information that is stripped of all identifiers except for zip codes and merely summarizes the claims submitted to the insurer/HMO.) In

this situation, the group health plan does not have to provide a notice of privacy practices to its enrollees and can, instead, let the insurer or HMO handle that aspect of complying with the regulation. And the employer/plan sponsor does not have to amend the underlying plan documents establishing the group health plan, a process that would be required if the employer/plan sponsor had greater need for access to protected health information. We anticipate that most group health plans will be structured so as to fall within these provisions, and we believe that employees of these employers/plan sponsors, at least those in larger organizations, should have little to fear in terms of privacy breaches.

Other provisions apply in circumstances where the employer/plan sponsor needs greater access to protected health information, such as arrangements where the employer/plan sponsor itself approves or pays for health claims. In that case, the group health plan is only allowed to disclose to the employer/plan sponsor information that is necessary for plan administration purposes. The group health plan cannot disclose any protected health information to the employer/plan sponsor until the group health plan receives a certification from the employer/plan sponsor that it has amended the underlying plan documents in very specific ways. Those plan amendments must include, among other things, (1) assurances that the employer/plan sponsor will comply with the regulation; (2) assurances that it will not use the information for employment-related purposes; (3) a description of the employees or classes of employees within the employer/plan sponsor that will have access to the information; and (4) a description of the firewalls that will separate the group health plan functions of the employer/plan sponsor from the rest of the employer/plan sponsor. Given the employer/plan sponsor's greater, and legitimate, need for protected health information, we believe the final regulation has done all it can to minimize inappropriate uses and disclosures by employers/plan sponsors.

While some may view these procedures as needlessly complex, we believe these safeguards are essential to protect privacy given HIPAA's failure to allow HHS to reach employers/plan sponsors directly and the genuine concerns of the public about access to personal health information by employers. By enacting a law that directly reaches employers, Congress could do more to alleviate employees' concerns about misuse of information by employers.

Protecting access to sensitive services

Individuals seeking sensitive health care services have a heightened concern that information about their medical condition or treatment may be inadvertently disclosed to others in their household, such as roommates, housemates, or family members (including parents in situations where a minor lawfully obtains a health care service without the consent or involvement of a parent). Disclosures could be made inadvertently by health care providers or health plans when they attempt to communicate with the individual at the individual's home, including the mailing of explanation of benefits (EOB) forms or bills to the individual or to the policyholder who is a family member of the individual (usually a spouse or parent). For example, a therapist's office might leave a message on the home message machine to remind a patient of an upcoming appointment and that message could be heard by anyone who resides in that household. A young woman who has seen the family's regular doctor for advice about family planning services might come home to find that a bill or EOB has been sent to her parents even though the minor has lawfully obtained those services without involving her parent. These types of communications can seriously compromise the privacy of an individual and may even deter the individual from seeking needed medical treatment.

The final regulation seeks to protect against these types of disclosures through section 164.522. This section provides for a right to request a restriction and the right to request that confidential communications be sent only through specified channels or means. While covered entities are not required to agree to requests for restrictions generally, health care providers must accommodate reasonable requests that communications to the individual be sent through alternate means or alternate locations. Health care providers are not allowed to require individuals to explain the basis for such a request. Health plans must accommodate such requests if the individual clearly states that disclosure of the information could endanger the individual. Unfortunately, we believe this "endangerment" standard is too strict. People who fear embarrassment, harassment, ridicule, or just verbal abuse may not meet that standard, and many will not want to come forward to explain their reasons at all. The regulation would better protect privacy if the standard that applies to providers also applied to plans.

Another important aspect of the regulation is the special treatment afforded to psychotherapy notes by section 164.508. These special provisions require an authorization for most uses and disclosures of psychotherapy notes, with stated exceptions.

Together, these provisions should give women of all ages seeking sensitive health care services greater control over how their information is used and disclosed. The special provisions that preserve the rights of minors are discussed below.

Right of minors

The National Partnership's comments to HHS on the proposed rule discussed at great length the need to preserve the rights of minors to confidential health care services. We were concerned that the final regulation not disrupt the status quo by giving parents access to sensitive information about adolescents that now remains confidential. Although we are pleased with the general approach taken with respect to minors, we are disappointed with the regulation's treatment of State laws that require or permit disclosures to parents.

The final regulation takes the general approach that the "individual" who is the subject of the protected health information exercises the rights provided in the regulation. The regulation also contains provisions allowing a personal representative to act on behalf of an individual in certain circumstances. Specifically, section 164.502(g) allows parents to be recognized as personal representatives of unemancipated minors. Under current law and practice, parents generally consent to care on behalf of their children and have access to their medical records (at least when anyone has access to those records). It is appropriate in such cases for parents to exercise the rights specified in this regulation.

But in many situations, information about a minor's receipt of health care services now remains confidential and is not shared with the parent without the minor's consent. It is appropriate in such cases for the minor to be the one to exercise the rights under this regulation. The final regulation keeps intact this delicate balance between parents and minors that exists in the real world today by recognizing three distinct circumstances under which unemancipated minors exercise their own rights. Those circumstances are the following:

When a minor's consent to a health care service is legally sufficient, regardless of whether the minor chooses voluntarily to involve a parent and that parent also provides consent;

When a minor may lawfully obtain care without parental consent, and the minor, a court, or someone else authorized by law consents; and

When a parent assents to an agreement of confidentiality between a minor and a health care provider.

This first provision is important because a minor who chooses voluntarily to notify or involve a parent should retain his or her right to exercise exclusively the rights of an individual under this regulation. Minors who can lawfully obtain care on their own often choose to involve a parent because of their close relationship with that parent. Because of this provision, this regulation will not operate as a disincentive to such voluntary parental involvement or to the sharing of confidences with the health provider by imposing as a consequence of such involvement the minor's loss of the right to control access to the personal health information related to that service.

The second provision is important because it preserves a minor's rights when the minor lawfully obtains a health care service without the parent's consent and the parent has not been involved at all.

The third provision preserves patient confidences in situations where a health provider such as a pediatrician and a minor patient enter into an agreement of confidentiality and the parent assents to this arrangement. Take, for example, a minor who visits the pediatrician with a parent for the purpose of a routine annual examination. Under protocols developed by the American Academy of Pediatrics, the pediatrician should raise with adolescent patients during their annual exams questions about risk-taking behavior such as drug or alcohol use and sexual activity. Typically, the parent provides the consent for the annual examination, but the pediatrician (again, under protocols developed by the American Academy of Pediatrics) explains to both the parent and the minor that the examination should be private and that the pediatrician will keep the minor patient's confidences. When and to the extent that the parent assents to this arrangement, a private and confidential examination follows. We are grateful that the final regulation will not upset these important, established protocols in the health care of adolescents.

These aspects of the final regulation strike the appropriate balance. They respect the important role that parents generally play in obtaining health care for their children, while at the same time recognizing the need to let minors continue to control their own protected health information in particular and narrow circumstances.

The final regulation protects minors in other ways. As discussed more fully below in the section on victims of violence, section 164.502(g)(5) gives covered entities the discretion to refuse to recognize a person as a personal representative in certain cir-

cumstances. This provision clearly applies to parents who seek to act as personal representatives on behalf of their minor children. This discretion allows the covered entity to act to prevent the minor from being endangered or subjected to harm. In addition, the final regulation (section 164.524(a)(3)(iii)) gives covered entities the discretion to refuse to provide a personal representative with access to an individual's protected health information in situations where access is reasonably likely to cause substantial harm to the individual or another person. This section also may be invoked to protect minors from harm.

While there are many provisions in the final regulation that preserve the rights of minors and protect them from harm, one policy judgment made by HHS in the final regulation is extremely troubling. The final regulation provides that State laws that authorize or prohibit disclosures of information about minors to parents are not preempted by the regulation. This approach to non-preemption is completely at odds with the approach taken elsewhere in the regulation. The general approach, which is required by HIPAA, is to preempt State laws that are contrary to the final regulation and less protective of an individual's privacy.

New protections for victims of domestic violence

The final regulation contains some extremely important provisions to protect the personal safety of victims of domestic violence, including children who are victims of abuse. The regulation recognizes that exceptions and allowances need to be made in situations where application of the general rules might put the individual at risk of harm. Of particular note are the following:

As discussed above, the final regulation allows victims of abuse (as well as others) to request that information not be used or disclosed in certain ways or be sent to their home. Together, these provisions should allow victims of abuse who have fled their abuser to keep their new address secret from their abuser, as well as allow victims of abuse to keep confidential the very fact of their medical treatment.

The final regulation gives adult victims of abuse, neglect, or domestic violence some power to object to disclosures about them to government authorities (including law enforcement officials). But disclosures required by law, as well as those expressly authorized by statute or regulation, are permitted even over their objection. Fortunately, section 164.512(c) also provides for notice to such victims in cases where disclosures are made without their knowledge or acquiescence. This will allow them to take extra measures to protect themselves against retaliation. The regulation does not require notice when the covered entity concludes, in the exercise of professional judgment, that providing notice would place the individual at risk of serious harm. The regulation also does not require notice when the notice would go to a personal representative whom the covered entity reasonably believes is responsible for the abuse, neglect or other injury, and the covered entity concludes, in the exercise of professional judgment, that providing notice to such person is not in the best interests of the individual.

The final regulation gives individuals the opportunity to object to disclosures of facility directory information and to disclosures to family members and friends of information directly relevant to the person's involvement in the individual's care. Section 164.510 requires the exercise of professional judgment in assessing the individual's best interests in situations where the individual is not present, is incapacitated, or an emergency prevents the covered entity from seeking the individual's permission. Although we would have preferred language in the text of the regulation about the potential of harm to the individual, at least the preamble to section 164.510 explicitly cautions covered entities to be alert to situations where disclosure to a possible perpetrator of violence could cause the patient harm. (Fed. Reg. at 82523, 82663)

The final regulation, in section 164.502(g)(5), gives covered entities the discretion to refuse to recognize a person as a personal representative in certain circumstances. This can occur when the covered entity believes that the individual has been or may be subjected to domestic violence, abuse, or neglect by the person requesting to act as personal representative, or that treating the person as a personal representative could endanger the individual. In either case, the covered entity can refuse recognition when, in the exercise professional judgment, it concludes that is not in the best interests of the individual for the person to be treated as a personal representative.

The final regulation, in section 164.524(a)(3)(iii), also gives covered entities the discretion to refuse to provide a personal representative with access to an individual's protected health information in situations where access is reasonably likely to cause substantial harm to the individual or another person. Unfortunately, the general requirement that covered entities explain, in writing, to the requestor (in this

case, the personal representative) the basis for the denial may result in harm to the very individual this exemption is designed to protect.

CONCLUSION

This privacy regulation is an important milestone in federal law. We believe that HHS has done an excellent job of reconciling the diverse interests of the various stakeholders, and we hope that Congress will not upset this balance. We urge Congress to fill in the gaps left by HIPAA, but we implore Congress not to unravel these new privacy protections. We also urge Congress to ensure that HHS has the resources that it will need to properly implement and enforce the regulation.

The CHAIRMAN. Our next witness, Dr. G. Richard Smith, is testifying on behalf of the Association of American Medical Colleges. He is at the University of Arkansas for Medical Sciences, where he is director of the Centers for Mental Healthcare Research. In addition to numerous professional activities during his career, he is at present a principal investigator on the Mental Health Services Research Centers Grant from the National Institutes of Mental Health and has published extensively in professional literature.

It is good to have you with us. Please proceed.

Dr. SMITH. Thank you, Mr. Chairman, and let me first say that I admire your stamina for being able to take testimony, and I appreciate you being here.

The CHAIRMAN. That is because it is so interesting and stimulating.

Dr. SMITH. I am a practicing psychiatrist, and I also conduct mental health services research. I am speaking today in behalf of the Association of American Medical Colleges. The AAMC represents the Nation's 125 accredited medical schools, over 400 major teaching hospitals and health care systems, more than 87,000 faculty and 92 professional and scientific societies, and the Nation's 67,000 medical students and 120,000 residents.

We wish to acknowledge our appreciation for the efforts of HHS to become informed about the daunting complexities of our contemporary system of health care delivery and payment and the critical importance to health research of access to archival medical information and to seek consultation and advice broadly throughout the rulemaking process.

The challenge for medical information privacy law or regulation is to find the appropriate balance between the competing interests of individual privacy and the compelling public benefits that flow from the use of medical information in providing care, in teaching, and in pursuing the Nation's biomedical, behavioral, epidemiological and health services research agenda.

My testimony will focus on the effects of the rule on medical and health education and research, about which we have grave concerns. However, the Association's members are responsible for operating the Nation's renowned teaching hospitals and health systems and for providing complex, cutting-edge medical care to all patients, including those covered by Medicare and Medicaid, and in disproportionate share, to those with no health insurance coverage at all. Thus, we are cognizant of the rule's enormous impact on treatment, payment, and health care operations, to use the rule's vernacular, and we wish to endorse the comments made here today by the American Hospital Association.

I will first turn my attention to teaching, although most of the testimony will be directed to research, where our concerns are especially acute.

The rule potentially negatively affects the teaching that can take place in our Nation's medical schools and teaching hospitals. The AAMC strongly urges the committee to request HHS to eliminate the rule's ambiguity about teaching. Failure to do so will seriously impair the quality of American health professions education, which is widely respected as the best in the world. It will also serve as a strong disincentive for community hospitals, clinics, and physicians to participate in health professions education at a time when both changing medical practices and medical pedagogy are placing increasing emphasis on the importance of such educational settings. The disincentive will result from the burden of having to apply the "minimum necessary" standard to each teaching interaction and from fears of liability for inadvertent violations of the rule.

The rule will have substantial effects on the conduct of medical and health research, and the effects of some of its provisions will, we fear, be most unfortunate. In particular, epidemiologists and health services researchers continue to depend upon the ready accessibility of archived medical records to collect the large and appropriately structured and unbiased population samples required to generate meaningful conclusions about the incidence and expression of diseases in specific populations.

Indeed, in the present climate of public concern about cost, quality, and efficiency of our rapidly changing health care system, and with the intensifying concern about health disparities within our increasingly multiethnic communities and the effectiveness and safety of novel drugs, devices and biologics in such populations, the need to promote and support large-scale retrospective epidemiological and health services research has become even more urgent a national priority.

The concerns about the rule's adverse effects on research are several and include the following. First, the AAMC believes that a great majority of the retrospective research with archived medical records could and should be performed with de-identified information, but that is only possible if the definition of "de-identified" is simple, sensible, and geared to the motivations and capabilities of health researchers, not to those of advanced computer scientists and cryptanalysts with mischievous or criminal proclivities.

Second, the AAMC is concerned about the lack of clarity created for obtaining a waiver for the requirement of specific authorization for research access to protected health information contained in archived medical records.

Third, the rule mandates a new set of patient rights, sometimes referred to as "fair information practices." That includes the rights to inspect, copy, and amend medical records and to obtain upon request a detailed record of each unconsented or unauthorized use or disclosure of protected information during the preceding 6 years. Unfortunately, the rule is internally inconsistent and will result in confusion and perhaps chaos in institutional review boards and privacy boards.

Finally, on the basis of the above concerns and because of the generally forbidding tenor of the rule, its complexities, ambiguities, burdens, costs, and hospitality to whistleblowers, the AAMC is very concerned that a particular unfortunate outcome may well be to encourage any covered entity for whom research is not part of the core mission to "lock down" its medical archives and refuse to make them accessible for research of any kind. Why should such an entity subject itself to the gratuitous costs, risks and liabilities that it could face from releasing protected medical information for any purpose other than those central to its core operations?

The AAMC commends the committee for convening this hearing to gather initial reactions to the effects of the new privacy rule. The Association urges the committee to be mindful of the fact that the facilitation of biomedical, epidemiological and health services research is a compelling public priority and has served this Nation well and offers bright promise for the future of human health.

It has been repeatedly noted that medical information is different from all other kinds of information that may exist about an individual—more personal, more private, more intimate and sensitive—and therefore that it needs higher protections. What has not been adequately recognized in the public debate is the essential and indeed irreplaceable role that medical information plays in a vast array of medical and health research that benefits all. That is a feature of medical information that is also different from any other kind of information about individuals, and it too demands protection.

The AAMC continues to believe that both the private and public goods that are inextricably entangled in medical information privacy policy would be best served by Federal legislation. Absent that, the Association has three recommendations.

First, Congress should direct HHS to reconsider the several provisions of the rule that we and others have identified today as troublesome.

Second, the compliance date, now set at 24 months from the effective date, is far too short and must be extended to at least 60 months, if not longer. The magnitude of the task of bringing the entire health care industry, especially the provider community, into compliance is daunting and cannot be managed in the 2-year window.

Finally, the cost of bringing the entire national health care system into compliance with the rule will be enormous, and the required resources cannot be generated within the health care enterprise alone. The AAMC believes that a creative Federal-State-private sector initiative, perhaps analogous to the concept of the postWorld War II Hill-Burton Act, will be necessary to reach this goal.

Thank you very much for the privilege of testifying.

The CHAIRMAN. Thank you, Dr. Smith.

[The prepared statement of Dr. Smith follows:]

PREPARED STATEMENT OF G. RICHARD SMITH, JR.

Mr. Chairman and members of the Subcommittee, I am Richard Smith, M.D., Professor of Psychiatry and Medicine at the University of Arkansas for Medical Sciences. I am a practicing psychiatrist and also conduct mental health services research. I lead the Centers for Mental Health Services Research at the University

of Arkansas, which is one of the nation's largest mental health and services research groups, as well as our College of Medicine's health services research program. I am a recent past member of the National Mental Health Advisory Council for the National Institute of Mental Health (NIMH). I also chaired the NIMH Initial Review Group for mental health services research, which reviews virtually all of the mental health services research grant applications submitted to NIMH.

I am speaking today on behalf of the Association of American Medical Colleges (AAMC). The AAMC represents the nation's 125 accredited medical schools, over 400 major teaching hospitals and health care systems, more than 87,000 faculty in 92 professional and scientific societies, and the nation's 67,000 medical students and 102,000 residents. The AAMC is committed to promoting integrity in all of the core missions of academic medicine - teaching, research, patient care, and community service - and has always underscored the over-arching importance of respecting patient autonomy and the privacy and confidentiality of individually identifiable medical information.

Accordingly, the AAMC has participated vigorously in the many failed efforts of past years to enact comprehensive federal law that would establish uniform national standards to protect the privacy of medical information and penalize its inappropriate and harmful misuse. The Association interacted intensively with the Department of Health and Human Services (DHHS) staff as they reluctantly undertook the awesome task of drafting the HIPAA-mandated medical information privacy rule. The AAMC wishes to acknowledge its appreciation for the efforts that DHHS made to become informed about the daunting complexities of our contemporary system of health care delivery, payment, and operations, and the critical importance to health research of access to archived medical information, and to seek consultation and advice broadly throughout the rule-making process.

The challenge for medical information privacy law or regulation is to find the appropriate balance point between the competing interests of individual privacy and the compelling public benefits that flow from the use of medical information in providing care, in teaching, and in pursuing the nation's biomedical, behavioral, epidemiological and health services research agenda. The Congress over many years of extraordinary bipartisan effort proved unable to find that balance; and not surprisingly, given the enormity of the task and the intensity of clashing values and passions with which the issues of individual privacy generally, and medical information privacy in particular, have become suffused, the Privacy Rule also fails.

The AAMC's testimony will focus on the effects of the rule on medical and health education and research, about which we have grave concerns. However, the Association's members are responsible for operating the nation's renowned teaching hospitals and health systems, and providing complex, cutting-edge medical care to all patients, including those covered by Medicare and Medicaid, and those with no health insurance coverage at all. Thus, we are very cognizant of the rule's enormous impact on treatment, payment and health care operations, to use the rule's vernacular, and we wish to endorse the comments made here today by the American Hospital Association (AHA). In particular, we agree with AHA that the rule is over-reaching; that it will be much more costly and burdensome than the rule's authors wish us to believe and will create an expensive new "privacy bureaucracy" that, absent sources of new funding nowhere yet identified, represents a substantial unfunded mandate; that it cannot be implemented effectively nation-wide within the 2-year compliance window specified; and that the inability of the rule to preempt state laws will prove to be increasingly problematic and burdensome, in an era in which individual mobility, interstate health care delivery, payment and operations, and interstate research are all commonplace.

While the bulk of our testimony will be directed to research where our concerns are especially acute, we will first make some brief comments about health professions education where a lack of clarity in the provisions of the rule is troubling. Teaching is referenced only three times in the final rule. The first occurs in Part 160.103 (Definitions) and asserts that "Workforce" includes "trainees and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." Although the word "students" is not mentioned explicitly, we assume that they are meant to be included in the category of "trainees." The second reference is in Part 164.501 (Definitions) and states that "Health care operations" includes "conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills. . ." The third and final reference is found in Part 164.508(a)(2), which specifies that authorization is required for any use or disclosure of psychotherapy notes (which receive special protections under the rule) except for already consented treatment, payment, or health

care operations, use by the originator of the notes for treatment, or (164.508(a)(2)(i)(B) use or disclosure in training programs.

Two features of the rule are especially consequential with respect to its effect on teaching. The first is the Standard: minimum necessary (164.502(b)), which requires that a covered entity limit the use or disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use or disclosure. The second is the extension of the rule's provisions (164.501 - "Protected Health Information") to all individually identifiable health information transmitted or maintained in any form or medium -electronic, written, or oral. One of the very few exemptions from the minimum necessary standard is for disclosures to or requests by a health care provider for treatment. In addition, the rule (164.514(d)(3)(iii)(C)) permits a covered entity to rely on the representation of a professional who is a member of the workforce that the protected health information requested is the minimum necessary for the stated purpose. Compliance with the standard for essentially all other uses or disclosures of protected health information must either be specified in the covered entity's policies and procedures when the uses and disclosures are routine or recurrent, or be dealt with individually on a case by case basis.

Since trainees are not defined in the rule as "health care providers" or "professionals," their use or disclosure of protected health information would be subject to the minimum necessary standard under the treatment exception and would not be permitted on the basis of the trainee's representation alone. Therefore, although the psychotherapy notes exemption might suggest that the rule takes a permissive stance with respect to students' access to and uses of protected health information, the fact is that nowhere does the rule explicitly allow disclosures of protected health information to health professions students which are not subject to the "minimum necessary" standard. The rule's ambiguity on this issue is a major concern for the AAMC, which believes strongly that the education of medical residents, medical students, nursing students, and other health professions students requires that their access to the medical information of their patients should be determined exclusively by their mentors in accordance with the needs of their respective educational programs. The AAMC supports the proposition that medical residents and medical and nursing students, as well as other health professions students, as necessary, should have unrestricted access to medical information of their patients access should be unrestricted—a proposition that the rule seems to recognize, peculiarly, only with respect to psychotherapy notes.

Currently, when a patient seeks medical care in a teaching setting, the consent form (that is, the traditional consent form, not the new consent required by the rule) typically includes a statement that the patient may be seen by health professions residents and students. It is also common practice that a patient's expressed wish not to be seen by students or residents is honored. The AAMC would prefer that these practices be permitted to continue, and that the traditional consent form language be incorporated into the teaching entity's Notice and (newly required) Consent for treatment, payment and health care operations, with a clear statement that students and residents will have full access to the medical information of their patients. A patient's objection should always be respected, as it is now.

The AAMC strongly urges the Committee to request DHHS explicitly to allow the sharing of protected health information within the content of accredited health professions educational programs. Failure to do so will seriously impair the quality of American health professions education, which is widely respected as the best in the world. It will also serve as a strong disincentive to community hospitals, clinics, and physicians to participate in health professions education, at a time when both changing medical practices and medical pedagogy are placing increasing emphasis on the importance of such educational settings and experiences. The disincentive will result both from the burden of having to apply the minimum necessary standard to each teaching interaction, and from fears of liability for inadvertent violations of the rule.

The rule will have substantial effects on the conduct of medical and health research, and the effect of some of its provisions will, we fear, be most unfortunate. The AAMC is disappointed that its strong objections to the relevant provisions in the proposed rule were largely ignored by DHHS. The Association has emphasized repeatedly in Congressional briefings and testimony, and in publications, the critical importance of access to archived medical records for a vast array of biomedical, behavioral, epidemiological, and health services research. We have pointed out that medicine has always been, and remains to this day, an empirical discipline, and that the history of medical progress has been created over the centuries from the careful, systematic study of normal and diseased individuals. From countless such studies has emerged our present understanding of the definition, patterns of expression and

natural history of human diseases, and their responses to ever improving strategies of diagnosis, treatment, and prevention.

In particular, epidemiologists and health services researchers continue to depend upon the ready accessibility of archived patient records to collect the large and appropriately structured and unbiased population samples required to generate meaningful conclusions about the incidence and expression of diseases in specified populations, the beneficial and adverse outcomes of particular therapies, and the medical effectiveness and economic efficiency of the health care system. Indeed, in the present climate of public concern about the costs, quality, and efficiency of our rapidly changing health care delivery system, and with intensifying concern about health disparities within our increasingly multi-ethnic communities and the effectiveness and safety of novel drugs, devices and biologics in such populations, the need to promote and support large scale, retrospective epidemiological and health services research has become even more urgent a national priority.

The AAMC's concerns about the rule's adverse effects on research are several and include the following:

First, the AAMC believes that a great majority of retrospective research with archived medical records could and should be performed with de-identified medical information, but that is only possible if the definition of "de-identified" is simple, sensible, and geared to the motivations and capabilities of health researchers, not to those of advanced computer scientists and cryptanalysts with mischievous or criminal proclivities. The Association has earlier commended the approaches to this problem taken in the Bennett and Greenwood bills, both of which sharply circumscribed the definition of "identifiable medical information" to information that directly identifies an individual, and of "de-identified medical information" to information that does not directly identify the identity of an individual. And both bills appropriately coupled these straight forward definitions with the criminalization of unauthorized attempts to re-identify individuals from such de-identified medical information. An apt descriptor for this approach to de-identification is "proportionality," in that the burden of preparing de-identified medical information is proportional to the interests, needs, capabilities and motivations of the health researchers who require access to it.

Unfortunately, DHHS has persisted in setting a single bar for "de-identification," and that bar is much too high. Thus, the standard for de-identification of protected health information (164.514) requires either that "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" must determine that the risk is very small that the information could be used alone, or in combination with "other reasonably available information" to identify an individual and "documents the methods and results of the analysis that justify such determination," or that 18 specific identifying elements are removed, including "geocodes" and most chronological data, that, in our judgment, would render the resulting information useless for much epidemiological, environmental, occupational and other types of population-based health research. Among the 18 elements to be removed are "device identifiers and serial numbers," which would make it impossible, for example, to use such information for post-marketing studies of device effectiveness or failure.

The AAMC continues to believe that the department's approach to de-identification is not only unfortunate but contrary to the dictates of sound public policy, which should be to encourage to the maximal possible extent the use of de-identified medical information for retrospective health research. Whatever an apt descriptor for the rule's treatment of this issue might be, it most certainly is not "proportionality". The Association urges the Committee to direct DHHS to rethink its approach to de-identification, and to create a standard that more appropriately reflects the realities of health research and the motivations and capabilities of health researchers, not of exaggerated fears of threats from lurking decryption experts. We also urge that revision of the standard should be accompanied by an unambiguous warning that unauthorized attempts at reidentification constitute a punishable offense. We remind the Committee that to our knowledge, there has never been a documented breach of the confidentiality of archived research records.

Second, the AAMC is deeply concerned about some of the new criteria created by the rule (164.512(i)(2)) for obtaining a waiver of the requirement for specific authorization for research access to protected health information contained in archived medical records. To begin, we wish to commend DHHS for persisting during the rulemaking process in its determination to define circumstances (164.512(i)(1),(2)) under which research access to archived medical records may be permitted without specific authorization, and to extend the reach of the new privacy protections to research that now falls outside the bounds of the Common Rule. The creation of Privacy Boards (PBs) closely modeled in structure and function on Institutional Review

Boards (IRBs) is sensible and to be applauded. We also commend the department's wise decision to allow covered entities to permit researchers access to protected health information without authorization or IRB or PB review when the purpose is (164.512(i)(1)(ii)) solely to review the information "as necessary to prepare a research protocol or for similar purposes preparatory to research," or (164.512(i)(1)(iii)) "solely for research on the protected health information of decedents."

The rule requires that the IRB or PB determine that all of 8 new criteria (164.512(i)(2)(i)(A)(H)), which are intended to be in addition to the provisions of the Common Rule and any requirements of state law that are more stringent, have been satisfied before it can approve a waiver of the requirement for specific authorization for access to protected health information for research purposes. Two of the new criteria appear to be internally contradictory: criterion (A) requires the determination that "[t]he use or disclosure of protected health information involves no more than minimal risk to the individuals," while criterion (E) requires determination that privacy risks are "reasonable in relation to the anticipated benefits . . . and the importance of the knowledge that may reasonably be expected to result from the research." We do not understand how a threshold determination of "no more than minimal risk" can be squared with a subsequent requirement to determine that risks are "reasonable" in relation to anticipated benefits and the importance of new knowledge. By what newly devised metric is an IRB or PB to weigh the "reasonableness" of risk that it has already determined is no more than minimal?

The AAMC finds the language of new criteria (B) and (E) inherently very troubling. Criterion (B) requires the determination that "[t]he . . . waiver will not adversely affect the privacy rights and the welfare of the individuals," while criterion (E), as already noted, calls for a balancing of privacy risks against anticipated benefits and importance of new knowledge. There are no objective metrics or normative standards that IRBs or PBs can use to measure "privacy rights" or 44 privacy risks," and the AAMC is very concerned at the prospect of requiring IRB or PB members to render judgments on the basis of nothing more than their personal belief structures or ideologies. The decisions of IRBs or PBs must inevitably rest upon individual judgments that are informed by professional knowledge and experience, and reached through rational discourse, debate, and sometimes, compromise. We fear that debates about privacy rights and risks may be of a very different sort and more closely analogous to debates about such deeply held beliefs as 44 animal rights" or "right to life," in which positions are based upon beliefs or ideologies, and compromise proves impossible to achieve.

The Association has repeatedly warned about the dangers of introducing into the IRB, and now the PB, process determinations for which there is no experience, received wisdom, or consensus within the scientific or lay communities to turn for guidance. Privacy rights and risks may be comfortable terms for ethicists, privacy advocates, and constitutional lawyers, but how are they to be weighed or balanced in the assessment of specific research proposals that may require access to hundreds or thousands or even more medical records, as the rule now requires? For most reviewers, the evaluation of privacy risks or dangers to privacy rights would most readily be

accomplished by examining the integrity of the confidentiality protections to be afforded the research files, such as those laid out in criteria (F), (G), and (H), with which the Association has no quarrel. But by listing the latter separately, the rule's architects clearly meant to distinguish them from the rights and risks that must be determined in criteria (B) and (E). We are very troubled by criteria (B) and (E) and urge the Committee to direct DHHS to reconsider its handiwork yet again, lest we find our IRBs and PBs mired in ideological gridlock that would make hollow the waiver provisions set out in this Subpart.

Third, the rule mandates a new set of patient rights, sometimes referred to as "Fair Information Practices," that includes the rights to inspect, copy, and amend medical records, and to obtain upon request a detailed record of each unconsented or unauthorized use or disclosure of protected health information during the preceding 6 years. The rights of individuals to inspect, copy and amend (164.524, 526) are expressly limited to protected health information in a "designated recordset." The rule (164.501) defines "designated record set" as a group of records maintained by or for a covered entity that includes medical, billing, enrollment, payment and related records, or is "used, in whole or in part, by or for the covered entity to make decisions about individuals." The rule defines "record" to mean "any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity."

The AAMC reads these definitions and the language of 164.524 and 164.526 as excluding research files created in research that does not include treatment from the right of access to inspect, copy or amend. For research that includes treatment

(i.e., clinical trials), the rights clearly do apply, except in very limited circumstances during the active conduct of the trial. However, the language in 164.528 (Accounting of disclosures) is different. It does not restrict protected health information to that in a designated record set, and therefore it applies to disclosures of any protected health information for research purposes. Considering the large numbers of medical records required, for example, in epidemiological and health services research, the burden of recording each and every research disclosure could easily become onerous and costly. It would be helpful to the research community and the entire health care enterprise if the department would clarify its intentions here and indicate whether the AAMC's reading of these provisions of the rule is correct.

We observe that the AAMC has consistently espoused the wisdom of maintaining wherever possible, formal and sharp distinctions between clinical and research records. This is primarily because the needs for and magnitude of access to these two different kinds of records, and, therefore, the ability to protect their confidentiality, are so profoundly different. Such distinctions, if generally applied and scrupulously maintained, would protect research records and archives that may contain elements of protected health information from the very burdensome and complex provisions mandated in this rule. Enforcing this distinction should be straight forward in retrospective, or secondary, research in which an investigator requires access to patients' records but has no direct interaction of any kind with the patients themselves. Even in interactive or interventional research, in which the research may involve treatment, maintaining the distinction is arguably worthwhile, even though more difficult, in order to protect the use and disclosure of research information that has nothing at all to do with treatment from being entangled in the rule's many requirements.

Fourth, the standard of "minimum necessary" applies to the disclosure of protected health information for research that will be performed under a waiver of specific authorization approved by an IRB or PB. In such instances, the rule requires the IRB or PB to determine that the information requested by the investigator meets the "minimum necessary" requirement. The AAMC is unclear about how IRB or PB members can possibly make this determination with any confidence in judging proposals that require access to very large numbers of medical records. We are very concerned that the expectation that the standard has been met will generate a substantial risk of liability not only for the covered entity, but for the M/PB members themselves, and discourage both IRBs/PBs from granting, and covered entities from acknowledging, waivers of authorization. This, in turn, makes even more discouraging the department's approach to the issue of de-identification, which, as we have explained earlier, will force many researchers who would not otherwise have chosen to do so to seek protected health information for their projects.

Finally, on the basis of the above concerns, and because of the generally forbidding tenor of the rule, its complexity, ambiguities, burdens, and costs, the AAMC is very concerned that a particularly unfortunate outcome may well be to encourage any covered entity for whom research is not part of the core mission to "lock down" its medical archives and refuse to make them accessible for research of any kind. Why should such an entity subject itself to the gratuitous costs, risks, and liabilities that it could face from releasing protected health information for any purpose other than those central to its core operations? And yet, access to medical archives in covered entities outside of academic medical centers is essential for many kinds of large, population-based epidemiological, health services, and public health research studies, as well as for post-marketing studies of the effectiveness and safety of approved drugs and devices. That the rule could produce an outcome of this kind is not inconceivable, although certainly not intended. It would be much sounder policy for the Committee to direct the department to reconsider these troubling provisions of the rule to ensure that such a tragic outcome does not occur rather than to deal with its aftermath.

The AAMC commends this Committee for convening this hearing to gather initial reactions to the effects of the new Privacy Rule. The Association urges the Committee to be mindful of the fact that the education of health professionals, as well as the facilitation of biomedical, epidemiological, and health services research are compelling public priorities that have served this nation well and offer bright promise for the future. The issues that surround medical information privacy are very difficult, as the Congress, and this Committee in particular, have learned in recent years. The DHHS has stated repeatedly that this nation needs a sensible, comprehensive, national standard of protections of medical information privacy that can only be accomplished through wise federal legislation. The difficult challenge for lawmakers and regulators alike is to find the correct balance between the need to protect the privacy rights of individuals and the many social benefits that flow from the appropriate use of medical information in teaching and research.

It has been repeatedly noted that medical information is different from all other kinds of information that may exist about an individual—more personal, more private, more intimate and sensitive, and therefore, that it needs higher protections. What has not been adequately recognized in the public debate is the essential, indeed, irreplaceable, role that medical information plays in a vast array of medical and health research that benefits all humankind. That is a feature of medical information that is also different from any other kind of information about individuals, and it, too, demands protection. The AAMC continues to believe that both the private and the public goods that are inextricably entangled in medical information privacy policy would best be served by federal legislation. Absent that, the Association urges the Committee to direct DHHS to clarify the regulations with respect to the ambiguities associated with training health professions students, and to rethink and revise those provisions that we believe pose serious threats to the vitality of biomedical and health sciences research that requires access to archived medical records. In addition, the AAMC supports the position of others in the health community that the 2-year implementation schedule is overly ambitious given the state of electronic information technology now in place in the health care delivery system.

Finally, irrespective of whether federal regulation or legislation is the chosen mechanism for protecting the privacy of medical information, the AAMC is convinced that the capital costs of developing and implementing nationwide the information technology systems required to bring the health care system into compliance will demand resources far beyond the capacity of the system to generate. Therefore, the AAMC suggests that a bold federal-state-private sector initiative, perhaps analogous to the post World War II Hill-Burton Act, will be necessary to reach this goal. The AAMC stands ready to work with other interested parties to help develop the agenda for this effort.

Thank you very much for the privilege of testifying before this Committee today.

The CHAIRMAN. Our final witness of the day, appearing on behalf of the Blue Cross/Blue Shield Association, is Mr. Robert C. Heird, senior vice president of Anthem Blue Cross and Blue Shield in Indianapolis. In this capacity, he is the executive sponsor of Anthem's Health Insurance Portability and Accountability Act Initiative. Mr. Heird has an undergraduate degree in business management from the University of Maryland, and he completed an advanced management program at Harvard Business School. He is on the board of directors of the Academy of Health Care Management.

It is a pleasure to have you with us today, Mr. Heird. We look forward to your testimony. You are the final witness of the day, and I will listen especially carefully.

Mr. HEIRD. Thank you so much, Mr. Chairman.

I realize that I am the only obstacle between you and lunch, so I will try to monitor your light system very closely.

Mr. Chairman and members of the committee, I am Bob Heird, senior vice president for Anthem Blue Cross and Blue Shield, testifying on behalf of the Blue Cross and Blue Shield Association.

Anthem Blue Cross and Blue Shield is a licensee of Blue Cross and Blue Shield Association. We have 7 million members in eight States—Connecticut, New Hampshire, Maine, Colorado, Indiana, Kentucky, Nevada, and Ohio. We have 15,000 associates who are also members and patients. So we appreciate the opportunity to testify here today.

Blue Cross and Blue Shield plans believe that there is a basic need for clear roles necessary to assure consumers that their health care is kept strictly private. For us, there is no question as to whether patient records should be kept private, but only as to how this should be done.

Our challenge is to view these roles through the eyes of our customers. Our members demand and expect superior service. The key question for us is whether this role meets our customers' expecta-

tions. And while we are still analyzing the hundreds of pages of the final rule, we have concluded that the rule does not provide the kind of value that our customers expect.

The rule is operationally infeasible, extremely costly, and would threaten quality improvement efforts throughout the health care system.

Therefore, we urge Health and Human Services to reconsider the final rule by providing for another comment period to allow time to identify and correct those serious problems in the final regulation that could harm consumers.

The final rule contains significant concerns, some of which are completely new from the proposed rule, that deserve more time for analysis and comment. Today I would like to highlight four of the top issues.

First, our customers want clear guidelines about where to direct questions and problems. Unfortunately, the final rule would layer new Federal rules on top of existing State laws. This would only add more red tape and frustration for everyone.

Consider for a moment the Anthem customer living in Lawrenceburg, IN who drives 15 miles to the Cincinnati-Northern Kentucky Airport, goes to work, and then drives another 15 miles to downtown Cincinnati, OH for treatment. Assume that there is an issue; what State rules—Ohio, Kentucky, Indiana? Is it HHS because of HIPAA? Is it governed by the law where the insurance policy is written? Is it governed by where the employee lives, or is it governed by where the provider delivers care? Our customers and the providers need to know their rights and whom to call.

Second, our customers want timely quality care, the kind of care that America prides itself on. The "minimum necessary" rule would require all of us to establish new processes and reorganize and redesign our operations so that we are only using and disclosing the minimum information necessary. This will require all of our efforts to ensure that patients receive the right care at the right time.

Simply put, this runs counter to the Institute of Medicine report that highlights the need for complete and timely access to patient information to prevent the wrong care.

Third, we are concerned that the business associate provisions are unworkable. Requiring business associates to establish procedures and notices consistent with the myriad of covered entities with which they contract will create an exponential number of differing standards of business associates.

Fourth, our customers want practical rules that facilitate their interaction with their doctors, hospitals, and health plans. We are concerned that the required consent provisions that apply to providers will have negative downstream effects on our customers. We are concerned about real life implications.

Consider for a moment the mother who calls her pediatrician on the telephone for advice on her sick baby. Her last visit was before the compliance date, and there is no consent on record. Does this mean the pediatrician cannot look at the child's record while on the phone?

What about a person calling on behalf of an elderly relative? Required consents could actually end up threatening our customers' quality of care and delaying the service that we provide.

Let me discuss cost briefly. And we will be clear—it will cost us to generate privacy protection. We are in favor of privacy protection, but it will be at a cost. The issue is whether or not the cost required will be an effective response to the need.

In addition, the high costs and other problems included in the privacy regulation are exacerbated by the HIPAA transaction and code-set regulations that were issued last year. The transaction regulations required doctors and hospitals and health plans to reorganize their operations, adopt new code-sets, and reengineer their computer systems in less than 2 years, and then, in addition to that, establish new privacy rules, all at the same time. In the end, the analogy has been made to Y2K; HIPAA will be more costly than our Y2K initiative.

We are asking that the implementation time frame for the transaction and code-sets regulations be extended by a 2-year period. Obviously, unless we do otherwise, we believe that there could be a system meltdown where claims and basic services are delayed or delivered incorrectly.

Thank you for the opportunity to testify today.

The CHAIRMAN. Thank you.

[The prepared statement of Mr. Heird follows:]

PREPARED STATEMENT OF ROBERT HEIRD

Mr. Chairman and Members of the Senate Committee on Health, Education, Labor and Pensions, I am Robert Heird, Senior Vice President for Anthem Blue Cross and Blue Shield, testifying on behalf of the Blue Cross and Blue Shield Association (BCBSA). BCBSA represents 46 independent Blue Cross and Blue Shield Plans throughout the nation that provide health coverage to 79 million—or one in four—Americans. As part of the Blue Cross and Blue Shield system, Anthem Blue Cross and Blue Shield provides coverage to more than seven million members in eight states including: Connecticut, Maine, New Hampshire, Colorado, Indiana, Kentucky, Nevada, and Ohio.

We appreciate the invitation to testify today on the final privacy regulations issued by the Department of Health and Human Services (HHS) on December 28, 2000. This testimony provides us the opportunity to view these regulations through the eyes of our customers—and to identify and discuss those issues that will have the most significant impact on them.

BCBSA believes that safeguarding the privacy of medical records is of paramount importance. We support a basic set of clear federal rules for the health care industry that assures all consumers their health information is kept strictly confidential. At the same time, we know that our members demand and value superior customer service. Any set of rules needs not only to allow for timely delivery and payment of health care services, but also minimize hassles and costs.

During the comment period following promulgation of the proposed rule, BCBSA submitted over 50 pages of detailed comments and recommendations. It is clear from the final regulation that HHS took into consideration many of our comments and sought a balance in the final rule.

However, despite their efforts, the regulation still needs significant revision. Without substantial changes, the regulation is likely to slow the delivery and payment of care to consumers and the providers who take care of them.

We are still analyzing the hundreds of pages of the final regulation. It is an extremely complex rule and we fear that we have only begun to scratch the surface in identifying critical problems. There are significant new provisions in the final rule—some of these represent improvements, but many other areas require more thought and opportunity for comments.

Because of our existing concerns and the need for further analysis, we urge the Department of Health and Human Services to reconsider the final rule by providing for another comment period to allow time to identify—and correct—those serious problems in the final regulation that would harm consumers. We are committed to helping HHS identify those problems and construct and implement a regulation that maximizes consumer protections, while preserving the ability of the health care system to provide efficient, quality services to consumers.

My testimony focuses on five areas: Background, Key Concerns with the Regulation, Positive Aspects of the Regulation, Cost of the Regulation, and Recommendations on Privacy

BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) provided HHS the authority to promulgate privacy standards for health information if Congress did not pass legislation by August 1999. The statute was very narrow and directed HHS to issue privacy rules to assure that information transmitted as part of the new HIPAA standardized electronic transactions would be kept confidential.

The final regulation would require covered entities (i.e., health plans, providers, and clearinghouses) to:

- Obtain new authorizations from consumers before using or disclosing information, except for purposes of treatment, payment, health care operations and other limited circumstances (providers would be required to obtain consent even for treatment, payment, and health care operations);

- Allow individuals to inspect, copy and amend much of their medical information;
- Track all disclosures made other than for treatment, payment and health care operations;

- Recontract with all business associates to require them to use and disclose information according to the new privacy rules;

- Institute procedures to assure that only the "minimum necessary" information is used or disclosed for a given purpose;

- Designate a privacy official and train staff;

- Follow specific rules before using protected health information for research; and

- Develop a host of new policies, procedures and notices.

In understanding the full scope and implications of the regulation, it is important to be aware of the following:

The Regulation is Not Limited to Electronic Records: The privacy standards under HIPAA were intended to apply to electronic transactions that are developed and maintained under the law's Administrative Simplification provisions. While the proposed rule's application to paper records was arguably ambiguous, the final rule clearly applies not only to electronic records, but also to any individually identifiable information "transmitted or maintained in any other form or medium."

The Regulation Affects Internal Uses of Information as Well as Disclosures: A common misconception regarding the regulation is that it regulates only the disclosure of information to a third party. In fact, the regulation has enormous implications for the use of information internally within an organization. This means that organizations will be required to comply with rules for internal treatment purposes, claims processing, utilization review and other routine health care purposes even though the information never leaves the organization's possession.

The Regulation Affects a Broad Array of Organizations and Information: The definition of "covered entity" is broad in scope—including not only doctors, hospitals and health insurers, but also employer health plans (insured and self-funded, except for self-administered plans with fewer than 50 participants), laboratories, pharmacists and many others. All organizations that service health care organizations that are not included specifically as a "covered entity" are indirectly subjected to the privacy rule through a provision that requires covered entities to contract with their "business associates." For instance, lawyers, auditors, consultants, computer support personnel, accountants and other non-health oriented organizations would fall into this category.

In addition, the definition of "protected health information" (PHI) is much broader than what most individuals consider their health information. The definition goes beyond an individual's medical records to include insurance records, oral information, and demographic data.

KEY CONCERNS WITH REGULATION

Our overall concern with the final regulation is that its intricate complexity will require a major reorganization of every doctor's office, hospital, pharmacy, laboratory, research facility, and health plan—as well as other organizations. We expect the final rule will lead to extremely costly infrastructure and procedural changes in each and every entity. For example, new sound-proof walls and offices may need to be built in health care facilities, new computer systems may need to be installed, and more lawyers and training personnel may need to be hired.

Although BCBSA has a number of concerns with the final rule, we have highlighted the four most problematic regulatory provisions in this testimony:

A. Dual Federal and State Regulation

The regulation layers a new comprehensive set of federal rules on top of an already existing complex patchwork of state privacy laws. The regulation follows the HIPAA regulatory construct in that state laws are preempted only if they are contrary to the regulation and are less stringent. In addition, the regulation specifically "saves" certain state statutes from preemption, such as those relating to health surveillance.

We know our customers want a clear understanding of their privacy rights. However, we are concerned that the intersection between state and federal privacy laws under the complex construct of the HIPAA regulatory model will create more red tape and frustration for health care providers and consumers. It will be unclear whom to call for resolution on specific rules—HHS or the states—and this lack of clarity will lead to more telephone calls, more steps, and more hassles for everyone.

Doctors, health plans and other covered entities must determine, on a provision by provision basis, which parts of state law would be retained and which would be replaced by federal law. This is further complicated by the necessity for rapid transfer of information in today's health care industry because of the mobility of patients. For instance, an individual may live in the District of Columbia, work in Virginia and visit a physician located in Maryland. Covered entities dealing with this individual will have to evaluate the interplay of three state statutes with the federal law. In addition, covered entities also must factor in the interplay of other federal laws relating to privacy. Even if each covered entity engaged an attorney to prepare a preemption analysis, different attorneys are likely to prepare conflicting interpretations—possibly leading to costly litigation with the states, the federal government and consumers.

This regulatory construct will be problematic for our customers. Instead of facilitating a member's ability to know his or her privacy rights, this complex preemption process is sure to confound that individual. First, individuals will be hard pressed to determine which aspects of the state and federal privacy laws apply to them, so it will be extremely challenging for them to determine if in fact, they have been wronged. In addition, consumers will not know where to direct complaints if they do feel that their rights are violated—Maryland? Virginia? The District of Columbia? The Secretary of Health and Human Services? It is likely that consumers will be bounced from one jurisdiction to the next until the consumer locates the one which has the law that has been violated—or the consumer becomes frustrated and gives up.

Our preference—and the clearest path for everyone in the system—would be for federal privacy law to preempt state law. Having a clear federal law would provide consumers and doctors with a clear path when answers are needed. However, we recognize that a complete preemption of state law is outside the statutory authority of HHS. Therefore, in our comments on the proposed rule, we recommended that HHS prepare a detailed privacy guide for each state explaining how existing state laws intersect with the new federal rules. We asked that the guide also address whether a privacy provision is triggered by a consumer's residence, location of provider or other criteria and that HHS prepare the guide in collaboration with state government officials. We also asked HHS to assure the guide incorporates other federal privacy laws, such as the Federal Privacy Act and Gramm-Leach-Bliley Act. As part of this process, we recommended that each individual state should certify agreement with HHS' analysis so everyone has a clear understanding of the rules.

We believe this legal guidebook needs to be prepared well in advance of implementing the final regulations. Doctors, health plans, and other covered entities will need this completed analysis before computer systems can be redesigned, forms and notices are changed, consumer brochures are modified and updated, and other procedures can be brought into compliance. Bringing plan and provider operations into compliance with these complex new regulations will consume a significant share of health care dollars. It is critical that these affected entities only have to modify systems and other items once.

Unfortunately, HHS failed to provide for this legal guide in the final regulation. In the preamble to the final regulation, HHS said that "many commenters" requested a similar state by state analysis. However, HHS declined to perform the analysis for the same reason they decided against a formal advisory opinion process: First of all, they indicated that "such an opinion would be advisory only" it would not bind the courts'. In other words, they felt that even with HHS guidance, there was no guarantee regarding final decisions or outcomes.

Second, HHS indicated that workload issues drove their decision against formal preemption guidance. The preamble says that "the thousands of questions raised in the public comment about the interpretation, implications and consequences of all of the proposed regulatory provisions have led us to conclude that significant advice

and technical assistance about all of the regulatory requirements will have to be provided on an ongoing basis—but we will be better able to prioritize our workload “if we do not provide for a formal advisory opinion process on preemption as proposed.”

We urge HHS to reconsider this decision and issue a state-by-state analysis prior to implementation of the final rule.

B. Minimum Necessary Standards

The regulation instructs doctors, health plans, and other covered entities to use or disclose only the minimum information necessary to accomplish a given purpose and discourages the exchange of the entire medical record. At first blush, this standard seems to be a perfectly reasonable, common sense provision.

However, we are concerned about how we can best operationalize this concept without creating significant unintended consequences. It is important to recognize that this standard applies to the use of information as well as disclosure, and that the definition of disclosure includes broad terms such as “provision of access to.”

This standard may require a massive reorganization of workflow as well as possible redesign of physical office space, and could jeopardize the quality and timeliness of patient care, benefit determinations and other critical elements of the health care system.

Many news accounts have inaccurately portrayed this provision as including an exemption for treatment purposes. HHS includes a very narrow exemption in the final rule—for “disclosures to or requests by a health care provider for treatment.” This exemption does not cover “use” of the information, nor does it cover “disclosures by” providers. As a result, the minimum necessary rules may still place artificial limits on the ability of doctors to use and disclose health information for critical treatment situations—threatening the overall quality of care.

A few examples of other potential problems with the minimum necessary rule include:

As part of the description regarding the minimum necessary standard, the regulation includes a strong discouragement regarding the release of entire medical records of patients. The complete exchange of medical information is absolutely critical to assuring a patient receives the right treatment at the right time. The recent Institute of Medicine report, “To Err is Human,” highlighted the medical mistakes that are common in our health care system today. The IOM report states that errors are more likely to occur when providers do not have timely access to complete patient information. Discouraging the sharing of complete medical records would make it more difficult to guard against these medical errors. One covered entity may determine that a subscriber’s prescription is not relevant to be released. Further down the line, that lack of information may impede clinicians’ decisionmaking. It is critical to use complete medical records for a variety of important quality assurance functions, such as accreditation and outcomes measurement.

It is well documented that fraud and abuse is a costly element of our health care system. The Medicare program as well as private health plans have made combating fraud and abuse a priority. However, the minimum necessary standard is likely to impede fraud detection, because fraud and abuse units may be accused of using more than the minimum information necessary. Any impediment to fraud detection would increase the cost to consumers. For instance, the sign-in sheets used in doctors’ offices are also used to verify that doctors are seeing the volume of patients they report for payment purposes. It does not appear that the privacy regulation would allow for these sign-in sheets to continue to be used.

Health plans and providers actually may be forced to redesign their facilities to comply with the minimum necessary standard. For instance, when visiting friends in maternity wards, there generally is a white board describing all of the patients and their medical needs. Any visitor may view the information on the board—a likely violation of HIPAA. Another example of potential renovation is an orthopedist’s office, where the x-ray lightboard is centrally located outside of the patients’ rooms for easy access by the physician. Anyone in the office could view these x-rays containing patient social security numbers or names. Would the regulation require these providers to renovate their facilities to comply with the regulation?

These are a few examples of the types of activities that could fall awry of the privacy regulation. If implemented, this could impose incredible costs on consumers—not just in dollars and cents—but in lives as well.

C. Business Associates

The business associate provisions of the regulation require that doctors, health plans and other covered entities use prescribed contract terms with all of their “business associates” to assure these associates follow the HHS privacy rules. Doc-

tors, health plans and other covered entities could be subject to civil monetary penalties if they "knew" of privacy violations by their business associates.

The contractual specifications included in the regulation compound the problems in the business associate framework. The rule requires business associates to use and disclose protected health information in accordance with the notice and policies and procedures established by the covered entity with whom they contract. Many business associates will contract with multiple covered entities—each of whom have their own set of notices and their own uses of health information. This will create an exponential number of differing standards for business associates.

The confusion is exacerbated because some organizations—like health insurers—are covered entities in some areas (e.g. a healthcare coverage provider) and business associates at other times (e.g. third party administrator). Keeping track of what kind of relationship and what contractual rules to follow with which organization will be very difficult, confusing and time-consuming.

For example, Anthem Blue Cross and Blue Shield has many different relationships with other organizations. Anthem plays the role of licensed insurer and third party administrator (TPA) for medical and dental plans. Anthem is a pharmacy benefits manager (PBM) as well. In some cases, Anthem would be considered a covered entity; in other cases we would be considered a business partner. In fact, in some cases, like when we perform coordination of benefits (COB) with other insurers, both Anthem and the other insurer would be acting as covered entities, not as business associates of each other. We would not only have to follow rules as a covered entity but a host of other organization's rules and procedures as their business associate.

The timeframe for renegotiation of contracts with business associates is also a significant problem. Health plans and other covered entities will have two years to update contracts in conformance with the privacy rule. Considering the multitude of relationships that we have with other organizations, we are concerned that two years is insufficient time to inventory all business associate relationships and renegotiate contracts. Moreover, if a contract lacks a unilateral agreement clause that allows the health plan to change the contract only with respect to the privacy rule's requirements, the entire contract could be opened up for renegotiation—a time-consuming process possibly involving discussions over new payment rates and other contract clauses.

And finally, we believe the business associate provisions are outside of the statutory authority of the Department of Health and Human Services. HIPAA clearly delineates the covered entities subject to HHS oversight: health plans, clearing houses, and providers conducting standard transactions. By attempting to indirectly regulate other organizations, we believe HHS acted beyond its regulatory authority.

D. Consent and Individual Restrictions

The final regulation requires health care providers to obtain consent before using or disclosing protected health information for treatment, payment or health care operations. In addition, it allows individuals to ask the provider to restrict the use or disclosure of certain health information.

We remain concerned that a requirement to obtain consent for treatment, payment and health care operations could unintentionally delay and impede routine operations that are essential to providing quality care and timely payment.

The regulation's transition rules allow providers to use and disclose information collected prior to the compliance date based on a patient's prior consent. However, if a provider has not obtained a new consent by the compliance date for treatment, payment or health care operations, he/she would be unable to use or disclose information collected after February 26, 2003 for that patient. The regulations anticipate that providers would simply obtain consents when patients arrived for treatment. The rule also states that consent forms obtained before the compliance date may meet the rule's requirements—however many providers may not have consents on record, and if they do they may not be for treatment, payment and health care operations—but only for one of these imperative functions.

Imagine that a mother is calling her pediatrician on the phone for advice on her sick baby. Her last actual visit was well before the compliance date and there is no consent on record. Does that mean the pediatrician cannot look at the child's medical record while on the phone? What about an individual calling on behalf of an elderly relative for clarification about a particular medication but with no consent for that individual to access information? Or requesting additional payment information where the historical consent on file was only for treatment? Would the gerontologist be gagged from responding?

If a provider obtains a new consent but it does not list "payment" or "health care operations", there may be downstream impediments for some routine operations because providers could only disclose information for treatment purposes. For in-

stance, claims may not be able to be paid, case management programs could suffer, and special pharmacy programs and other programs that benefit consumers also could be impaired because disclosures for these purposes depend on consent forms including treatment and health care operations.

III. POSITIVE ASPECTS OF THE PROPOSED REGULATION

Clearly, we believe there are significant issues in the final regulation. However, HHS did address many comments in the final regulation in their effort to balance operational impacts with the overall goal of privacy.

A few of the most positive elements in the final regulation include:

"Statutory" Consent for Treatment, Payment and Health Care Operations for Health Plans: The regulation does not require a new consent for treatment, payment, and health care operations for health plans. We believe a "statutory" consent, meaning that covered entities may use or disclose protected health information without consent as a matter of law, is imperative.

Requiring health plans to obtain a new consent from current members would require numerous mailings and phone calls from health plans—a process akin to a "late bill" collections process—in order to obtain the new consents. In the interim, members and providers would experience delays in payment and other services.

Improved Definition of Health Care Operations: The final regulation includes a modified definition of what constitutes "health care operations" that reflects many of the comments received by HHS. The definition is critical since items encompassed within it are exempt from new authorizations and tracking of disclosure requirements that would create obstacles to conducting essential health plan activities.

We are pleased that HHS has incorporated many important and routine health plan activities into the final rule's definition. For example, we believe the definition may now allow health plans to continue many of their beneficial disease management and other quality improvement programs. The new "business management and general administrative activities" category will facilitate routine plan operations such as security activities, data processing and general maintenance. The "business planning and development" category will help plans to continue to develop more cost-efficient services and products.

No Third Party Liability in Business Partner Contracts: The final rule deletes the requirement that makes individuals third party beneficiaries of business associate contracts. We support deletion of this clause since HHS did not have the authority to create a new private right of action. The third party liability clause was not only beyond the scope of HHS' authority, but it would have left health plans and other covered entities exposed to substantial liability for breaches of privacy by business associates.

IV. THE COST OF THE REGULATION

BCBSA supports a basic set of privacy rules for the health care industry that assures consumers that their health information is kept private. We recognize that assuring consumer privacy involves additional resources. For us, the question is not whether privacy will generate costs, but whether the costs are more than they need to be. We believe a new final rule could be structured in a way to provide our customers with a better value.

HHS estimated the proposed regulation to cost \$3.8 billion over five years. HHS updated its cost estimate in the final rule to be almost \$18 billion over ten years—more than double its estimate for the proposed rule. However, we believe HHS' cost estimates continue to be understated. In response to the proposed regulation, BCBSA commissioned Robert E. Nolan Management Consulting Company to provide an independent estimate of several key provisions of the proposed regulation. The Nolan estimate is more than \$40 billion over five years in added costs for health plans, providers and other members of the health care community. We believe most of these costs remain applicable to the final privacy regulation.

BCBSA looks forward to working with Congress and HHS to restructure the regulation to provide a better value to our customers.

V. RECOMMENDATIONS

While we continue to analyze this complicated rule, our specific recommendations to date are:

(1) Provide a Detailed Analysis on Preemption of State Law (A Road Map for Consumers): While we recommend a full preemption of state law in the privacy area, we understand that it is outside of the statutory authority for HHS. In the absence of full preemption, we recommend HHS, working with the states, prepare a detailed

analysis of state and federal law to provide a clear guide on all provisions affecting the health care industry.

It is critical that this guidance is available at least two years prior to the compliance date of the regulation. Bringing operations into compliance with these complex new regulations will be expensive, so it is critical that doctors, health plans, and other covered entities only have to modify systems and other items once.

(2) Change the Minimum Necessary from Legal Standard to Guiding Principle: While we believe the minimum necessary standard is a laudable goal, we are concerned that it would be extremely difficult and expensive to implement this standard operationally and comply with it as a legal standard. Therefore, we recommend that HHS ask organizations to include the minimum necessary standard concept only as a guiding principle, not as a legal standard.

(3) Remove Business Associate Provisions. The business associate provisions should be removed from the regulation because they are: Outside of the Secretary's statutory authority; Confusing and create unnecessarily expensive relationships between doctors, health plans, and other covered entities; and Unnecessary since the vast majority of protected health information is maintained by organizations that are covered by the regulation.

At a minimum, we feel the business associate provisions should be changed as follows: Covered entities should not be considered business associates of each other; and Covered entities should be given at least three years to re-negotiate contracts and come into compliance with the business associate provisions.

(4) Provide a Statutory Consent for Health Care Providers: In the proposed rule, HHS recognized some of the operational problems of requiring authorization forms for treatment, payment and health care operations. We agreed with HHS' views, but recommended that covered entities be given the flexibility of requesting authorizations for treatment, payment and health care operations. The proposed rule would have actually prohibited it, unless required by State or other law.

We are pleased that the final rule retains a statutory consent for treatment, payment and health care operations for health plans, with the flexibility to request a consent if desired. However, we have concerns that the final rule requires health care providers to get consent for these essential functions. We feel that required consent may lead not only to operational issues, but could also affect treatment activities and quality of care.

(5) Include Additional Funding for Medicare Contractors and other Government Programs. We also urge congressional appropriators to factor the additional cost of privacy compliance into budget development regarding the Medicare fee-for-service contractors, Medicare+Choice plans, the Federal Employees Health Benefit Program, and other federal programs.

VI. CONCLUSION

Once again, we appreciate the opportunity to testify before you on this critical issue.

We would like to continue working with you, and the Department of Health and Human Services, on crafting privacy rules that meet our common goals of protecting consumers, improving quality, and minimizing costs.

The CHAIRMAN. I was just thinking how naive Senator Dodd and I were some 3 or 4 years ago when we decided that we could do all of this ourselves and come up with the perfect piece of legislation. We thought there would be a couple of problems with law enforcement and the abortion question, but wow, were we naive.

But it is a pleasure to have you here today and this panel especially to help us make sure that in the final analysis, we will have done a good job, because it is so critical and so important to all the people involved. So I very much appreciate your testimony.

Judith, let me start with you. You mentioned that you support the final rule's creation of a fire wall that creates separation between the plan sponsor or employer and the group health plan. However, I wonder if this separation can even be achieved, particularly for small employers, where it is not unusual for one person to make the employment decisions as well as all the human resources and benefits decisions.

Are you concerned that this provision will be difficult if not impossible for small employers to comply with?

Ms. LICHTMAN. We are very worried, and that is why I said in my statement that HHS did as much as they could given their legal authority under HIPAA, and it would therefore be up to Congress to pass legislation that ensured that employers were indeed covered entities, because I think that that is the only way to protect all employees. I think that HHS did the best they could with the hand they were dealt under HIPAA, but there is no doubt that we clearly want employers to be covered for privacy protections.

The CHAIRMAN. Dr. Smith, please explain the potential problems in health professionals training that may result when the "minimum necessary" standard is imposed on medical and nursing students.

Dr. SMITH. First, we believe that the rule is ambiguous. My students and my residents need to have access to the records of my patients and their patients, not just a portion of them. If there are ambiguities in the rule, legal counsel for my teaching hospital will impose certain restrictions that may limit, let us say, a nursing student from seeing the record of my patient. That nursing student needs to have access to the full medical record in order to be able to learn from that case that is a part of the hospital or a part of my practice. If he or she is participating in the care, they need to have access to that record.

The rule is ambiguous and contradictory in places, and we would urge that HHS look at that and that you encourage HHS to look at that and try to clarify that ambiguity.

The CHAIRMAN. Mr. Heird, you gave a cost estimate of \$40 billion over 5 years for the proposed rule. HHS has estimated that the final rule will cost approximately \$18 billion over 10 years. What do you believe the actual cost of the final rule will be, and how do you think these differences came about?

Mr. HEIRD. Senator, the final rule obviously is just out, and one thing that we are engaged in doing presently is a gap analysis of how the requirements of the final rule line up with our current practices. Until that is completed, we are not going to know for sure all of the implications.

We do note that there are systems requirements, as was discussed in the last panel, in order to track consent. There will be significant training implications required of all of our associates to understand consent, to understand "minimum necessary."

Our Association retained Robert E. Nolan Associates to do the analysis for us, and even though that was based on the proposed rules, we think that that number is essentially correct. Regretfully, we are not going to be able to tell you an exact number until we complete our gap analysis, but we think that that number is far more accurate than the original HHS estimates.

The CHAIRMAN. I am aware of insurance companies that are now offering integrated products to employers that consist of health insurance, disability insurance, and workers' compensation components. Since the product is integrated, I do not know if it is covered by the final rule, which covers health plans but not disability plans or workers' compensation. Does your company offer these types of

products, and would you be able to continue offering these products under the final rule?

Mr. HEIRD. We do have a broad set of product offerings. We are a pharmacy benefit management company, and part of our organization deals with the types of services that you mention. We are examining our organization now to determine exactly how impactful all of this will be, whether or not there are fire walls that will be required.

We know that in some cases, our organization will have to issue business associate agreements with outside organizations, but we also know that for our customers who are self-insured, we will be their business associate. So on the one hand, we will be the issuer of those agreements, and on the other hand, we will receive them. That is part of the complexity that we see with regard to the business associate process and our ability to be effective in the marketplace.

The CHAIRMAN. Ms. Lichtman, the public ultimately will pay the cost of implementation of the regulation by covered entities, whether through higher health care premiums or higher taxes or lost benefits. At what point do the financial costs outweigh the increase in privacy protection, and what if the burden of compliance is too great on small providers?

Ms. LICHTMAN. I think it is a fair question. I think it may, however, be a premature one. I note that HHS projects over 10 years a cost saving. Sitting here today, before February 26, it is hard for me to second-guess those cost savings projections, turn them into some nightmare of burgeoning costs, and answer your question about the cost-benefit analysis, which I think is a fair one.

I just think that if indeed I take their figures at face value—and I do—your fears may never be realized, and therefore, I may never have to get to the nightmare trade, and I think we need the experience to see that, and we will have plenty of time, including the very ample 2-year implementation time, to respond to that.

I also want to say something very quickly. It seems to me that HHS acted in a very responsible way in promulgating the final rule. They got 52,000 comments. Now, I am not an expert counter of comments, but that seems to me to be no small potatoes. The covered entities responded to that proposed rule and had quite ample opportunity to do so, so the final reg that HHS authored was in effect informed by the concerns and the comments of the covered entities, and HHS took those into account when they issued the final rule. I do not think that this committee or the Senate should lose track of what I believe to be a very reasoned approach to the final reg.

The CHAIRMAN. Please, Mr. Heird.

Mr. HEIRD. Thank you. I believe the earlier speaker from the American Hospital Association put his finger on a key issue, and that is that about 70 percent of the transactions that we receive today for claims are already automated. So the estimated savings we are not sure will exist from the transaction and code-sets part of HIPAA, because basically, we are going to go back through and redesign already existing systems. Every transaction—all the codes that make these electronic things work will have to change.

So we are not convinced that there is a savings there. If there is, we are completely unconvinced that there is a savings that equals the cost of privacy.

Having said that, I want to come back to my testimony, which was that we support privacy; the issue is how. We are concerned with the approach that we read in the regulations that that cost is disproportionate to the real value received.

The CHAIRMAN. Dr. Smith.

Dr. SMITH. Senator, if I might, our academic medical center, if we do a really good job this quarter, might break even, as opposed to losing money, which we have done for the last 20 quarters. Even if this thing costs a fraction of what people here are estimating, it is an awful lot for academic health centers that are struggling to keep their doors open.

One thing that I think HHS may have overlooked is what is the cost, as one of the speakers said, to some of the safety net providers—and we are not a small safety net provider; we are a very large safety net provider, but we provide the bulk of the uninsured care for the State of Arkansas that is at least a secondary or tertiary care level. These are quite expensive regulations that could impede operations and impede the ability to give people the care that they need.

The CHAIRMAN. Dr. Smith, please discuss your concern that health care providers whose core mission is not research may “lock down” their medical archives and refuse to make them accessible for research purposes. How serious a problem do you see that as being?

Dr. SMITH. In our work, for instance, we would do research about the effectiveness of treatment for depression in the State of Arkansas or across the South, for instance, and we might have to deal with not only getting our records, but we might have to deal with 15 or 20 insurance companies. So I might have to go to the Blue Cross and Blue Shield in Arkansas that has 60 percent of the market, and if Blue Cross and Blue Shield in Arkansas said, Gee, guys, this is too expensive for us—even though it is a good idea, our general counsel tells us that the risk of giving you protected information is too great, and therefore, we are not going to participate—then I cannot do my study, or my faculty cannot do the study, so we cannot actually find out what is wrong with the delivery system in Arkansas about providing care for people with mental disorders.

The comment that Senator Wellstone made earlier about the mentally ill—in a similar vein, I think that some of these provisions might actually cause providers not to give care if they have to go through extra hoops in order to protect the confidentiality of psychiatric diagnoses.

The biggest problem that we have in primary care is the fact that doctors do not recognize the disorders and do not treat the disorders because they say it is too much trouble, which to me is a crime, but if we make it worse, I have grave concerns about the health impacts of these rules.

The CHAIRMAN. Mr. Heird, do you have a comment?

Mr. HEIRD. I think the case was well made by Dr. Smith.

The CHAIRMAN. Ms. Lichtman.

Ms. LICHTMAN. Something strikes me that I think is important to say when we look at costs. There is a huge cost to society and to the GNP, if you will, if consumers, if patients, if human beings do not avail themselves of good-quality health care because of fears of their lack of privacy. That is a cost. So when we figure out how much it costs to implement these privacy regs, we also have to figure out how much does it cost us as a society not to have privacy regs in place, because there is a cost to us.

The CHAIRMAN. Dr. Smith?

Dr. SMITH. I would agree with Ms. Lichtman, and I think Ms. Goldman also made that same point. If people are not getting care because they are afraid of the violation of privacy, we do need good privacy regulations in order to ensure that people get the care that they need.

The CHAIRMAN. Mr. Heird?

Mr. HEIRD. I think that we are in violent agreement that privacy standards are required, and we all want them. Everyone in this room is a patient, and we all have a role to play in the delivery of health care and the financing of health care. So we all want clear and understandable rules. The question is how are we going to go about that in a way that we all think is an appropriate outcome for the common desire that we have.

The CHAIRMAN. My instincts tell me that this is an unusual moment, and we ought to sanctify it by concluding the hearing at this point with all three of you in agreement.

So thank you for very excellent testimony. We deeply appreciate all the work that has gone into your testimony, and we will still reserve the right to submit a few more questions to you.

[Additional statements and material submitted for the record follow:]

PREPARED STATEMENT OF SENATOR FRIST

Thank you, Senator Jeffords, for holding this hearing to examine the final regulation on medical records confidentiality released by the Department of Health and Human Services (HHS) last year.

The issue of privacy is a critical one to the American people, who have long valued the concept of individual privacy—and in no area is it more important than when it touches upon an individual's most sensitive medical history and information.

I don't need to remind anyone of the history of this issue. Legislation regarding the privacy of medical records has been debated ever since the computer age of the 1960s where concern was expressed that the electronic transfer of data jeopardized the privacy of personal information. The passage of the Federal Privacy Act of 1974 was one of the first attempts by Congress to protect personal information and records held by the federal government. But a comprehensive, federal law protecting one's medical information has eluded us before now. Today, even though Congress was unable to pass comprehensive medical privacy legislation, forcing the Secretary to write the regulations before us, the issue remains of utmost importance.

If there is any one sentiment to which I think we would all agree, it is that the regulations before us demonstrate exactly why there should be comprehensive Federal medical records privacy leg-

isolation—so that we may address what has become a confusing swamp of State laws, regulation, and court cases regarding the protection of health data. I am concerned that, despite its intent, this regulation may exacerbate this problem.

Now, throughout our efforts in the past several years, I worked from two overriding principles. First, and foremost, the main reason a health record is generated is for the care of the patient. The patient must remain our central focus—patients must feel comfortable in sharing personal information with their providers to receive the highest quality of care. Moreover, we must preserve the doctor-patient relationship—a relationship built on patients' trust in their providers.

Second, as a physician and researcher, I cannot overstate the importance that these efforts promote and support ongoing public health and medical research initiatives taking place throughout the country, and I will be looking to make sure that the regulations appropriately balance the confidentiality concerns with the need to foster our public and private research enterprise.

Our efforts to report and track infectious diseases through our public health system are vital to the health of all Americans, and they must be continued. Medical research using information gleaned from medical records has produced incalculable benefits to patients by improving our understanding of disease and health outcomes.

Access to health information is critical to ensuring public health, promoting medical/epidemiological/health outcomes research, improving the quality of care, and eliminating fraud and abuse from our health care system. These activities have a direct impact on patient care. We should not inadvertently harm patients by unduly restricting research efforts and halting advances.

The confidentiality of medical information is an extremely important issue to the American people—one that deserves our continued attention and thorough consideration. I look forward to today's testimony and to working with my colleagues on this issue in the coming months.

STATEMENT OF THE AMERICAN COUNCIL OF LIFE INSURERS

This testimony on the final Privacy of Individually Identifiable Health Information Regulation (the Regulation) of the Department of Health and Human Services (the Department) is submitted to the Senate Health, Education, Labor, and Pensions Committee (the Committee) on behalf of the American Council of Life Insurers (the ACLI). The ACLI is a national trade association whose 435 member companies represent 73 percent of the life insurance and 86.9 percent of the long term care insurance in force in the United States. The ACLI also represents 73 percent of the companies that provide disability income insurance. The ACLI commends the Department for its tremendous effort in crafting this vitally important rule and commends the Committee for holding this hearing. The ACLI appreciates the opportunity to submit testimony.

The ACLI strongly supports the Regulation's underlying goal of protecting individually identifiable health information. Life, disability income, and long term care insurers understand their responsibility to protect their customers' health information. ACLI member companies are strongly committed to the principle that individual have a legitimate interest in the proper collection and handling of their medical information and that insurers have an obligation to assure individuals of the confidentiality of this information. Several years ago, the ACLI Board of Directors adopted the "Confidentiality of Medical Information Principles of Support." These Principles were recently strengthened to provide for ACLI support for prohibitions on the sharing of medical information for marketing and for determining eligibility for credit.

The ACLI believes that the Regulation's goal of protecting individually identifiable health information may be achieved in a manner consistent with the significant public interest in maintaining the life, disability income, and long term care insurance markets which meet the private insurance needs of millions of American consumers. By their very nature, the businesses of life, disability income, and long term care insurance involve personal and confidential relationships. However, insurers selling these lines of coverage must be able to obtain and use their customers' health information in order to perform legitimate insurance business functions. The performance of these functions is essential to insurers' ability to serve and fulfill their contractual obligations to their existing and prospective customers. The ACLI

has attempted to analyze the final Regulation with a view toward the need to balance the goals of protecting the confidentiality of individuals' health information with life, disability income, and long term care insurers' need to obtain and use that information in order to issue, service, and administer insurance policies sought by individuals.

The ACLI and its member companies are still in the process of analyzing the Regulation and its effect on member companies' ability to engage in ordinary insurance business activities. The following reflects concerns with the Regulation which have been identified as of the present time. It is possible that the ACLI and its member companies may discover additional concerns as they continue to study the Regulation.

It is already clear that the Regulation will have a significant and direct impact on the manner in which life, disability income, and long term care insurers do business. Although life and disability income insurers are not "covered entities" under the Regulation, their ability to obtain individually identifiable health information, critical to the performance of basic insurance functions, such as underwriting and claims evaluations, will be subject to and determined by the Regulation's disclosure requirements and limitations. This is true because life and disability income insurers often must obtain individually identifiable health information from health care providers which are "covered entities" under the Regulation and which may only disclose protected health information as permitted thereunder.

Long term care insurers are covered entities under the Regulation. As such, they are subject to the full gambit of the Regulation's requirements regarding access, use and disclosure of individually identifiable health information. In addition, like life and disability income insurers, long term care insurers' ability to obtain individually identifiable health information from other covered entities (which are health care providers) is subject to the Regulation's disclosure limitations and requirements.

The ACLI has noted a number of changes which were made in the final Regulation in response to concerns raised by the ACLI in connection with the proposed regulation's disclosure requirements. However, there continue to be very troublesome ambiguities in some of the provisions of the final Regulation which could be construed to limit covered entities' disclosure of individually identifiable health information to life, disability income, and long term care insurers. This would limit these insurers' access to and use of health information which is critical to their ability to perform fundamental insurance business functions, such as underwriting and claims evaluations.

The ACLI recommends that the Regulation's current effective date of February 26, 2001, be delayed so that these ambiguities may be clarified. Clarification of these ambiguities would prevent the unintended consequences of restricting legitimate insurance business practices which are essential to life, disability income, and long term care insurers' ability to serve and fulfill their contractual obligations to their prospective and existing customers.

Below are more detailed explanations of the manner in which life, disability income, and long term care insurers use protected health information and ambiguities in the Regulation which could be construed to jeopardize legitimate and essential uses of that information by life, disability income, and long term care insurers.

WAYS IN WHICH LIFE, DISABILITY INCOME, AND LONG TERM CARE INSURERS USE INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

The process of risk classification is a system of classifying proposed insureds by level of risk. It enables insurers to group together people with similar characteristics and to calculate a premium based on that group's level of risk. Those with similar risks pay the same premiums. Risk classification provides the fundamental framework for the current private insurance system in the United States. It is essential to insurers' ability to determine premiums which are: (1) adequate to pay their customers' future claims; and (2) fair relative to the risk posed by proposed insureds.

The price of life, disability income and long term care insurance is generally based on the proposed insured's gender, age, present and past state of health, possibly his or her job or hobby, and the type and amount of coverage sought. Much of this information is provided directly by the proposed insured. Depending on the proposed insured's age, medical history, and the amount of insurance applied for, the insurer may also need information from the individual's medical records. In this event, when the insurer's sales representative takes the consumer's application for insurance, he will request that the applicant sign an authorization, provided by the insurer, authorizing the insurance company to: (1) obtain his health information from his doctor or from a hospital where he has been treated; and (2) use that information to, among other things, underwrite that individual's application for coverage.

Based on this information, the insurer groups insureds into pools so that they can share the financial risk presented by dying prematurely, becoming disabled, or needing long term care.

If a company is unable to gather accurate information or have access to information already known to the proposed insured, an individual with a serious health condition, with a greater than average risk, could knowingly purchase a policy for standard premium rates. This is known as adverse selection. While a few cases of adverse selection might not have a significant negative impact on the life, disability income, or long term care insurance markets, multiple cases industry-wide would likely have such an effect. This would be particularly true if individuals were to be legally permitted to withhold or restrict access to medical information significant to their likelihood of dying prematurely, becoming disabled or requiring long term care. The major negative consequence of adverse selection would be to drive up costs for future customers which could price many American families out of the life, disability income, and long term care insurance markets.

Most life and long term care insurance and much disability income insurance is individually underwritten. As part of the underwriting process, insurers selling life, disability income, and long term care insurance rely on an applicant's individually identifiable health information to determine the risk that he or she represents. Therefore, medical information is a key and essential component in the process of risk classification.

Once a life, disability income, or long term care insurer has an individual's health information, the insurer controls and limits who sees it. At the same time, insurers must use and disclose individually identifiable health information to perform legitimate, core insurance business functions. Insurers that sell life, disability income, and long term care insurance must use individually identifiable health information to perform essential functions associated with an insurance contract. These basic functions include, in addition to underwriting, key activities such as claims evaluation and policy administration. In addition, insurers must also use individually identifiable health information to perform important business functions not necessarily directly related to a particular insurance contract, but essential to the administration of servicing of insurance policies generally, such as, for example, development and maintenance of computer systems.

Also life disability income, and long term care insurers must disclose individually identifiable health information in order to comply with various regulatory/legal mandates and in furtherance of certain public policy goals such as the detection and deterrence of fraud. Activities in connection with ordinary proposed and consummated business transactions, such as reinsurance treaties and mergers and acquisitions, also necessitate insurers' use and disclosure of such information. Life, disability income, and long term care insurers must disclose individually identifiable health to: (1) state insurance departments in connection with general regulatory oversight of insurers (including regular market conduct and financial examinations of insurers); (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), concerned with insurers' market conduct; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations. Limitations on these disclosures would operate counter to the consumer protection purpose of these disclosure requirements.

Life, disability income, and long term care insurers need to (and in fact, in some states are required to) disclose individually identifiable health information in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies, state insurance departments, the Medial Information Bureau (MIB), or outside attorneys or investigators who work for the insurer. Again, any limitation on an insurer's ability to make these disclosures would undermine the public policy goal of reducing fraud, the cost of which is ultimately borne by consumers.

AMBIGUITIES RAISED BY THE FINAL REGULATION

As noted above, the final Regulation contains a number of ambiguities which could be construed to impose limitations on covered entities' disclosure of protected health information to life, disability income, and long term care insurers. This would limit these insurers' access to information essential to the performance of fundamental insurance business functions, particularly underwriting. As a result, these ambiguities are very troublesome.

One provision of the Regulation permits a covered entity to disclose an individual's entire medical record if the disclosure is "specifically justified." However, another provision of the Regulation provides that "(w)hen . . . disclosing protected

health information . . . , a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the . . . disclosure . . . " While it appears to be the intent of the Regulation to permit a doctor or hospital to release a proposed insured's entire medical record to a life insurer for the purpose of underwriting an application for life insurance coverage on that individual, it is not clear.

The provisions described above give rise to ambiguity and raise a number of questions particularly when they are considered in the context of possible disclosures of protected health information by covered entities to life, disability income, and long term care insurers. What is the nature and the level of justification required to "specifically justify" a covered entity's disclosure of an individual's entire medical record? What provision ultimately governs a covered entity's disclosure of protected health information—that governing disclosure of an entire medical record or that requiring a minimum necessary determination? Covered entities are not required to limit disclosures of protected health information to "the minimum amount necessary" when the disclosure is made pursuant to an authorization meeting specified requirements. How does or should that exception impact disclosures by covered entities to life, disability income, or long term care insurers submitting authorizations meeting those specified requirements?

The preamble to the proposed regulation correctly noted that "In certain circumstances, the assessment of what is minimally necessary is appropriately made by a person other than the covered entity . . ." It went on to explain that one of these circumstances arises when an individual authorizes a use or disclosure. The preamble noted that "In such cases, the covered entity would be unlikely to know enough about the information needs of the third party to make a 'minimum necessary' determination." This would be particularly true in the case of life, disability income, and long term care insurers which generally submit authorizations to covered entities on behalf of individuals seeking insurance coverage or payment of claim for insurance benefits. Moreover, it is the insurer, not the disclosing covered entity, which bears the economic risk in the transaction in connection with which the information is sought. It would be unfair to give a party other than the party bearing the risk the right to determine what information is the minimum amount necessary.

It appears that the drafters of the Regulation recognized and did not intend for the minimum amount necessary rule to be applicable to disclosures by covered entities to life, disability income, and long term care insurers. However, this is not entirely clear. Given its potential significant and adverse impact on the risk classification process, this ambiguity is extremely troublesome to ACLI member companies.

The Regulation also requires that a covered entity permit an individual to request that the covered entity restrict uses or disclosures of protected health information to carry out treatment, payment, or health care operations. The effect of these agreements on disclosures by covered entities to life, disability income, and long term care insurers is, again, unclear. If a covered entity health care provider makes such an agreement, it must adhere to it. Thus, if a provider has agreed not to disclose certain health information, it is unclear if that information could be disclosed to an insurer underwriting a life, disability income, or long term care insurance policy.

It is particularly troublesome that there is no requirement that covered entities indicate that any information is being withheld pursuant to such an agreement. As a result, material information about an individual, which may have been critical to fair and complete underwriting, may be withheld from an insurer underwriting an application for insurance coverage on that individual, without the insurer even being aware that any information is being withheld.

A number of the ambiguities described above are likely to have arisen because the Regulation was drafted with health care providers and health plans in mind and without a great deal of focus on the effect of the Regulation on entities, such as life and disability income insurers, which are not covered entities, but which would be significantly impacted by the Regulation. Again, the ACLI recommends that the Regulation's current effective date of February 26, 2001, be delayed so that these and other ambiguities may be clarified. Such clarifications will help avoid unintended consequences of restrictions on legitimate and essential insurance business practices.

Again, the ACLI appreciates the opportunity to submit this Testimony, and would be glad to answer any questions in relation to it.

CONFIDENTIALITY OF MEDICAL INFORMATION—PRINCIPLES OF SUPPORT

Life, disability income, and long term care insurers have a long history of dealing with highly sensitive personal information, including medical information, in a professional and appropriate manner. The life insurance industry is proud of its record of protecting the confidentiality of this information. The industry believes that individuals have a legitimate interest in the proper collection and use of individually identifiable medical information about them and that insurers must continue to handle such medical information in a confidential manner. The industry supports the following principles:

Medical information to be collected from third parties for underwriting life, disability income and long-term care insurance coverages should be collected only with the authorization of the individual.

In general, any redisclosure of medical information to third parties should only be made with the authorization of the individual.

Any redisclosure of medical information made without the individual's authorization should only be made in limited circumstances, such as when required by law.

Medial information will not be shared for marketing purposes.

Under no circumstances will an insurance company share an individual's medical information with a financial company, such as a bank, in determining eligibility for a loan or other credit—even if the insurance company and the financial company are commonly owned.

Upon request, individuals should be entitled to learn of any redisclosure of medical information pertaining to them which may have been made to third parties.

All permissible redisclosures should contain only such medical information as was authorized by the individual to be disclosed or which was otherwise permitted or required by law to be disclosed. Similarly, the recipient of the medical information should generally be prohibited from making further redisclosures without the authorization of the individual.

Upon request, individuals should be entitled to have access and correction rights regarding medical information collected about them from third parties in connection with any application they make for life, disability income or long-term care insurance coverage.

Individuals should be entitled to receive, upon request, a notice which describes the insurer's medical information confidentiality practices.

Insurance companies providing life, disability income and long-term care coverages should document their medical information confidentiality policies and adopt internal operating procedures to restrict access to medical information to only those who are aware of the these internal policies and who have a legitimate business reason to have access to such information.

If an insurer improperly discloses medial information about an individual, it could be subject to a civil action for actual damages in a court of law.

State legislation seeking to implement these principles should be uniform. Any federal legislation to implement the foregoing principles should preempt all other state requirements.

STATEMENT OF THE AMERICAN PSYCHIATRIC ASSOCIATION

The American Psychiatric Association (APA), a medical specialty society that represents 40,000 psychiatric physicians nationwide, appreciates the opportunity to provide a statement to the Senate Health, Education, Labor and Pension Committee for this hearing on privacy. We believe that patient privacy remains one of the key issues before the Congress.

Chairman Jeffords, Senator Kennedy and Committee members, we thank you for your continued commitment to protecting medical records privacy and for holding this hearing to determine whether the recently released Medical Privacy Regulation adequately serves the American public.

In recent years, as changes in technology and health care delivery have outpaced statutory, common law and other traditional protections that have ensured patient confidentiality, the level of privacy enjoyed by patients has eroded dramatically. It is certain that the new medical privacy regulation was badly needed. Similarly, one would hope that the privacy issues could be simply and easily agreed upon, but unfortunately the recent debates on medical records privacy have become too divisive. In our review of medical privacy, the APA believes that privacy issues should be debated based on the fundamental issue that the privacy regulations must safeguard the rights and the freedoms of those that need them the most. Who are these people? They are you, your families, your constituents, the elderly and the sick. They are the people that turn to the medical community to help them when they

or their family members are in need of medical treatment. Their dependence on the medical system is built on trust. They want to tell their physicians their closely guarded secrets and fears and trust that the medical system will support and care for them. Furthermore, it is not about those in need having to fight the system. The patient and their families have little time or energy or resources to argue over the legal loopholes or the fine print on privacy consent forms.

The Medical Privacy Regulation that was issued in December 2000 is a landmark rule because it is the first federal protection for health information. Moreover, a review of the regulation shows a significant but incomplete step on privacy. The APA feels that the regulations contain positive provisions as well as significant problems. In particular, there are issues with patient consent, marketing and fundraising loopholes, law enforcement provisions, business associates and costs.

CONSENT

The APA is pleased the final regulations require an individual's consent before their medical record can be disclosed for treatment, payment, or other health care operations. This section is necessary to allow patients to provide consent to release their medical records. The APA feels these provisions clearly define areas where consent is required.

However, the APA is concerned the regulations allow for a blanket consent at the time of entry into a health plan. This blanket consent means a patient is authorizing subsequent disclosures of personal information without knowing the type of information allowed to be disclosed, or who can receive this information. While the regulations allow the patient to revoke this consent, the regulations do not protect the patient from being dismissed from the plan for doing so. The patient should have the ability to revoke the consent at any time. The APA feels the rule does not adequately provide this patient protection.

The APA is supportive of the provision that a covered entity, which means health plans, health care clearing houses, and health care providers, needs to obtain a higher level authorization for any use or disclosure of psychotherapy notes. Psychotherapy notes may not be disclosed without the patient's specific authorization. Nonetheless, the APA feels the regulations fail to protect the whole psychiatric record that may contain as much sensitive information as the psychotherapy notes. The regulations change the current standard of practice relevant to the psychotherapy documentation provision

MARKETING AND FUNDRAISING

The APA is very concerned about a marketing and fundraising loophole that exists in the regulation. A patient's authorization is not needed to make a marketing communication to a patient if: it occurs face-to-face; it concerns products or services of nominal value; and it concerns the health-related products and services of the covered entity or of a third party and meets marketing communication requirements. For example, a marketer could knock on the door of a pregnant woman and try to sell her a product or service. Under the fund raising loophole a covered entity may use or disclose patient's demographic information and dates of health care to a business associate or to an institutionally related foundation, without a patient's authorization. Although, the covered entity must include in any fund raising materials it sends to a patient a description of how the patient may opt out of receiving any further fund raising communication. The APA maintains that the patient should be able to opt out before the fund raising communication is sent. For example, a commercial fund raising organization for a health facility could use confidential information about a Governor being a patient at that facility without the Governor's consent for use in their fund raising. The APA is particularly concerned about the need for sensitivity with psychiatric patient's names. Commercial fund raisers should not be allowed to take advantage of patients especially those with mental illness.

The regulations allow for the disclosure of health information without a patient's authorization for: public health activities; victims of abuse; fraud and abuse investigations; judicial and administrative proceedings; law enforcement purposes; decedents; research purposes; to avert a serious threat to health or safety; for specialized government functions; and workers' compensation. The APA believes in the intent of these provisions but feels the provisions for law enforcement, judicial and administrative proceedings, and specialized government functions are too intrusive and overly broad.

LAW ENFORCEMENT PROVISIONS

The APA is concerned about the provisions for law enforcement. The provisions permit disclosures in response to administrative summons and subpoenas issued by an investigating authority without an independent review by a neutral magistrate to determine whether the request should be granted or denied. The neutral magistrate is needed to guarantee a patient's privacy rights, which in turn prevents the potential prejudices or abuses by law enforcement. In fact, the neutral magistrate is an added safeguard that protects the integrity of the system and ensures that the medical records are reviewed by an independent judiciary official. The APA has strongly advocated for the courts to be involved in judicial review for obtaining medical records.

SPECIALIZED CLASSES (MILITARY, STATE DEPARTMENT AND OTHERS)

The APA is concerned the special rules in this section are overly broad and do not provide adequate procedural protections for patients. The consent of the individual should be the rule for the use and disclosure of governmental employees' medical records. Particularly objectionable are the provisions allowing broad access without patient consent for use and disclosure of medical records of Foreign Service personnel and their families. If such information is not evident from an individual's employment performance and history, these provisions seem to represent an invitation to discriminate against individuals with mental and other disorders.

COSTS

The APA believes the estimated costs imposed on small psychiatrist's offices for the first year of \$3,703 and consecutive years of \$2,026 seem unrealistically low. Psychiatrists will experience significantly higher costs and will have a heavy administrative burden, such as getting satisfactory assurances from a business associate through a written contract, keeping psychotherapy notes separate and locked from the rest of the psychiatric record, and providing written notice of their privacy practices to their patients. Similar to small health plans, small physician offices should be allowed to have 36 months for compliance to spread the cost over a longer period of time.

BUSINESS ASSOCIATES

Business associates with respect to covered entities means a person who performs a function or activity involving the use or disclosure of medical information on behalf of a covered entity including claims processing, billing etc. A business associate is not a member of the workforce of the covered entity. The regulations do not require covered entities to name patients as "third party beneficiaries" in contracts with business associates. Under this provision, the covered entity has a duty to mitigate any known harmful effects of a violation of the rule by a business associate. Surprisingly, a covered entity may avoid sanctions under the regulations, but be subject to negligence actions because of a business associate's violations—even in cases where the covered entity discovers the business associates' violation and takes steps to address the violation. We believe this provision shifts an unnecessary and potentially complicated administrative burden on a covered entity to completely list and thoroughly document the satisfactory assurance from a business associate through a written contract.

RIGHT TO ACCESS

The APA supports the provision where a covered entity may deny an individual access to inspect and obtain a copy of protected health information when the access is reasonably likely to endanger the life and physical safety of the individual or another person provided the individual is given the right to have such denials reviewed.

MINIMUM NECESSARY STANDARD

The APA supports the final rule retaining the "minimum necessary" standard of the proposed rule. The standard requires covered entities to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request for health information. This provision can be cited when dealing with unreasonable health plan requests for information. This standard does not apply for treatment purposes between providers.

MORE STRINGENT STATE LAWS

The APA is pleased the regulations establish a federal floor and a state law that relates to privacy of health information and is more stringent than the final regulation prevails over the federal regulation. Many states have more stringent laws for certain information such as mental health, genetic testing and sexually transmitted diseases. The stronger privacy protections would control.

CONCLUSION

In conclusion, we think the privacy regulations are needed but some provisions are inadequate to protect our patients. Our members as physicians take an oath first stated by Hippocrates that "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick—I will keep silence thereon, counting such things to be as sacred secrets." In order to make sure that doctor-patient confidentiality continues to protect patients in the new millennium.

Many parties were disappointed at how protective these regulations are of patient privacy and—in support of their own interests—will be arguing for surrendering many of the protections that patients have just gained. We encourage Congress and the administration not only to stand firm on these issues, but also to take this opportunity to extend the scope of privacy protection so necessary to effective medical care.

We thank you for this opportunity to testify, and we look forward to working with the Committee on medical records privacy issues.

STATEMENT OF JUDGE DAVID L. BAZELON, CENTER FOR MENTAL HEALTH LAW

On December 20, 2000, the U.S. Department of Health and Human Services issued the first comprehensive federal rule protecting the privacy of individuals' medical records, as required under the 1996 Health Insurance Portability and Accountability Act (HIPAA). These rules are particularly important for those whose medical record contains highly sensitive information which might be used against them should it fall into the wrong hands. In the case of mental health records, even the mere fact of having received treatment can result in discrimination in employment, financial dealings and other aspects of life. These rules are, therefore, particularly welcome by mental health consumers and their advocates.

This statement on the new health privacy rule is submitted on behalf of the Judge David L. Bazelon Center for Mental Health Law, a legal advocacy organization formed in 1972 and concerned with mental disability policy. Through precedent-setting litigation in the public-policy arena and by assisting legal advocates across the country, the center works to define and uphold the rights of adults and children who rely on public services and ensure them equal access to health and mental health care, education, housing and employment.

This is a strong rule, with many protections for consumers, including those who use mental health services. The Bazelon Center is extremely pleased that it sets a floor for privacy protection, but does not pre-empt any state laws that give greater privacy protection, including laws already enacted by states and statutes that may be enacted in the future. Accordingly, states are still free to add more protections and to improve privacy protections. In a world with fast-changing information systems, this flexibility for states is crucial.

The regulations give individuals who use health care services new rights, which will be especially important for those who use mental health services because of the great potential for discrimination in many aspects of life stemming from the stigma and misunderstanding about mental illness. In particular, we strongly endorse the following rights granted to individuals through this regulation:

The right for individuals to know how their medical records will be used and, in general terms, to whom medical information will be disclosed.

The right to give informed consent before providers can use or disclose one's health care information, even for routine purposes such as treatment, payment and the operation of a health plan. Since providers may condition treatment on the consumer's providing that consent and health plans are permitted to seek and obtain informed consent and may condition enrollment on consent to the sharing of information for the purposes of treatment, payment and health care operations, this right does not infringe on the need for providers and plans to act in their own interest.

The right to request restrictions on uses or disclosures of their information (such as requesting that information not be shared with a particular individual). The provider or health plan may decide if it will honor this request, thus balancing once

again the rights of the individual and the administrative burden on providers and plans.

The right to request that communications from the provider or plan be made in a certain way (such as prohibiting phone calls to the individual's home). This request must be honored unless it is unreasonable and creates an undue administration burden. This is extremely important for highly sensitive information, such as mental health information.

The right to see and copy their own health information and to be provided documentation on who has had access to this information. We strongly support the provision that individuals may be denied access to their records only when the access would endanger the life or physical safety of any individual.

The right to request amendment to their record if it contains incorrect information.

As a result of these new federal rules, all consumers will receive from their provider or health plan a notice of rights to health-information privacy, which will be extremely informative for consumers. We support the requirements for the content of these notices which is included in the regulation.

However, we are disappointed that the rule permits individuals to be contacted for marketing and fund-raising purposes, although we appreciate that this activity is limited under the rule and that consumers are given the opportunity to opt out of further communications of either type.

The rule also sets appropriate limits on the sharing and disclosure of information in a medical record and we strongly endorse the following provisions:

Information shared must be limited to the minimum necessary to accomplish the intended purpose of the use, except if information is shared for treatment purposes, when the entire record can be shared.

Health plans and providers are given incentives to create and use information that does not disclose the consumer's identity (de-identified information).

Providers and health plans must establish privacy-conscious business practices to protect health records—e.g., training employees, designating a "privacy officer" to assist individuals with complaints and ensuring that appropriate safeguards are in place to protect the privacy of information.

Special protections are provided for highly sensitive mental health information shared during psychotherapy. Psychotherapy notes may not be disclosed without the consumer's specific written authorization and health plans may not condition enrollment or eligibility for benefits on the individual's providing this authorization. Providers may also deny their patient access to psychotherapy notes, since the notes are entirely private information to be used only by the therapist herself.

The rules restrict the use of health information by employers so that self-insured employers may not use health care information for purposes unrelated to health care, such as making personnel decisions.

Health information developed in research studies will also be protected. The requirement that IRBs review both privately-funded as well as publicly-funded research is welcome, as we believe there is no rationale for separate and lower standards for some research. We also note with approval that the rule adds new criteria that IRBs must apply in making their decisions.

One area where we are concerned that protections are too weak is that of sharing information with law enforcement officials. Providers and health plans are permitted to share information with law enforcement officials when these officials have obtained a court order, court-ordered warrant or subpoena, or through an administrative request. The administrative request may be obtained without a judge's review and in some cases can be written by the law enforcement officer him- or herself. Although in the case of an administrative request, the rule includes some restrictions with respect to relevance of the information and the need for specificity, there is no judicial oversight. Also, the rules permit the release of information when police are trying to identify a suspect, allowing the police to browse through identifiable health care information. This is of concern.

We are also concerned about that part of the rule that permits sharing of health information in civil litigation. No judicial review is necessary before one party to litigation may subpoena medical records based on an assertion that they are relevant to the case. Records can also be released in response to a discovery request or other legal processes with no specific court order. As with law enforcement, some restrictions apply, but there is considerable flexibility for access to private health information when this is seen as necessary by the parties involved in civil litigation or during criminal proceedings. Given the potential harm if mental health information becomes public knowledge, we are concerned that the rule does not provide sufficient protection here.

Health information may also be disclosed for necessary public health activities, such as for prevention or control of disease, child abuse or neglect, domestic-violence reporting and quality control of products. Health information may also be disclosed for various activities related to health care oversight, including audits, administrative procedures and licensure. We support these provisions.

The Bazelon Center is concerned about how these rules will apply in public mental health systems. Generally speaking, we are pleased with the Department's decisions to include Medicaid plans under the rules. State Medicaid programs are considered "health plans" in the context of these regulations and must operate as such, protecting the privacy of information in the same way a private health plan. Medicaid providers must, similarly, follow these same rules.

However, the new federal privacy rules do not automatically apply when services are provided entirely through grant funds. Therefore, when state or federal grants fund a particular mental health service (as when a state passes federal block grant funds on to a community mental health center) only some of the protections in these new rules will be in place. While mental health providers will be required to adhere to the rules regarding notification, consent, sharing of information, sharing only the minimum of information necessary for a specific purpose, etc., information collected by the state or county agency that gives the grant may not be as well protected as information collected by a private health plan or a Medicaid agency. The rule is not specific on how a granting agency must protect information, and officials in the Department of Health and Human Services have informed us that final decisions on how the rules will or will not apply when services are funded through a grant will be made through a process of interpretation. As of this date, these interpretative guidelines have not been issued; accordingly, this remains a gray area. We hope the committee will encourage the department to answer these important questions. The Bazelon Center is greatly concerned that state and local mental health systems have accurate and useful information systems so that decisions on public sector spending can be informed by good data. However, such systems must also protect the privacy of individually-identifiable health information.

Thank you for the opportunity to submit our views.

MENTAL HEALTH LIAISON GROUP,
WASHINGTON, DC, 20005,
February 20, 2001.

Hon. Jim Jeffords,
Chairman,
Committee on Health, Education, Labor, and Pensions,
U.S. Senate,
Washington, DC 20510.

DEAR MR. CHAIRMAN: This letter is submitted on behalf of the Mental Health Liaison Group for inclusion in the Record of the Hearings on Medical Records Privacy, held by the Committee on Health, Education, Labor and Pensions of the United States Senate, on Thursday, February 8, 2001.

The 36 organizations listed below, as consumer, family, advocate, professional and provider organizations concerned about the confidentiality of medical records, strongly support the regulations recently issued by the Department of Health and Human Services. These new rules represent an historic and important step, and are urgently needed in this era of electronic innovation and of mergers which create large health care entities. These trends heighten the need for policies and procedures that will protect individuals from the inappropriate sharing of their personal health information. The potential for abuse of highly sensitive information, such as information on mental health treatment, is enormous. We are only too aware of the many individuals whose lives have been ruined by the sharing of such information, and have growing concern about those who are delaying or avoiding treatment for fear of such disclosures. Due to the discrimination which frequently follows disclosure of mental health treatment, the protection of mental health medical record information is a critical concern.

It is particularly important that these new rules not only set a uniform national floor for privacy protection, but also do not pre-empt any state laws that give greater privacy protection. States are thus free to act promptly in response to the rapidly-changing world of information technology and to address state-specific issues.

We are also extremely pleased to see the following protections in the proposed new rule:

The right to know how one's medical records will be used and, in general terms, to whom medical information will be disclosed.

The opportunity to give informed consent before health care information can be used or disclosed even for routine purposes such as treatment, payment and the operation of a health plan.

The right to request restrictions on uses or disclosures of health information (such as requesting that information not be shared with a particular individual).

The right to request that communications from the provider or plan be made in a certain way (such as prohibiting phone calls to the individual's home).

The right to see and copy one's own health information, with the exception of psychotherapy notes, and to be provided documentation on who has had access to this information and the right to request amendment to the record if it contains incorrect information.

The rules also provide special protections for highly sensitive mental health information shared during psychotherapy. Psychotherapy notes may not be disclosed without the consumer's specific written authorization and health plans may not condition enrollment or eligibility for benefits on the individual's providing this authorization. We had strongly urged that such a protection be included in the rule for this uniquely private and highly sensitive information. Therapists must have the freedom to document their conversations with patients in a separate protected part of the medical record and this information is not necessary for purposes of payment and health care operations.

We are also extremely supportive of the provisions which provide for appropriate privacy practices in health care settings, such as:

Limiting information shared to the minimum necessary to accomplish the intended purpose of the use, except if information is shared for treatment purposes, when the entire record can be shared.

Incentives for health plans and providers to create and use de-identified information.

The requirement that providers and health plans establish privacy-conscious business practices to protect health records, such as training employees, designating a "privacy officer" to assist individuals with complaints and ensuring that appropriate safeguards are in place to protect the privacy of information.

We are also pleased to see that the rules restrict the use of health information by employers so that self-insured employers may not use health care information for purposes unrelated to health care, such as making personnel decisions. Again, because of the significant possibility of discrimination, such a barrier between those who need information in order to run an efficient health plan and other staff of the employer is a critical protection for mental health information.

We also support the provisions requiring that health information developed in public and private research studies be reviewed by Institutional Review Boards (IRBs). We also note that the rule adds new criteria that IRBs must apply in making their decisions. The rule also appropriately permits health information to be disclosed for necessary public health activities, such as for prevention or control of disease, child abuse or neglect, domestic-violence reporting and quality control of products.

One area where we are concerned that protections are too weak is that of sharing information with law enforcement officials. Information can be shared with law enforcement officials in response not only to a judge's order but also through an administrative request. This administrative request may be obtained without a judge's review and in some cases can be written by the law enforcement officer him- or herself. We are similarly concerned that information can be shared in civil litigation without judicial review. For example, the rule permits records to be released in response to a discovery request or other legal processes. In this regard, courts have ruled that plaintiffs waive the psychotherapist-patient privilege when claiming emotional distress or placing their mental condition at issue.

However, we are disappointed that the rule permits individuals to be contacted for marketing and fundraising purposes. Although we appreciate that this activity is limited under the rule and that consumers are given the opportunity to opt out of further communications of either type we strongly believe that personal health information should never be shared for the purposes of marketing or fundraising.

However, despite some areas of concern, we are generally extremely pleased with the final rule. Its most significant weaknesses are in areas where the Department did not have the authority to act. We strongly urge Congress to consider legislation that would ensure that individuals have the right to act when their health care privacy has been violated, by providing for a private right of action. Only Congress can create this right, without which there will continue to be little recourse for those whose rights have not been protected in accordance with this rule.

Thank you for considering our views.

Sincerely,

Alliance for Children and Families, American Association of Pastoral Counselors, American Association of Private Practice Psychiatrists, American Association for Marriage and Family Therapy, American Board of Examiners in Clinical Social Work, American Counseling Association, American Family Foundation, American Federation of State, County & Municipal Employees, American Group Psychotherapy Association, American Mental Health Counselors Association, American Psychoanalytic Association, American Psychological Association, American Society of Clinical Psychopharmacology, Anxiety Disorders Association of America, Association for Ambulatory Behavioral Healthcare, Association for the Advancement of Psychology, Bazelon Center for Mental Health Law, Children and Adults with Attention-Deficit/Hyperactivity Disorder, Clinical Social Work Federation, Employee Assistance Professionals Association, Federation of Behavioral, Psychological and Cognitive Sciences, Federation of Families for Children's Mental Health, Legal Action Center, National Alliance for the Mentally Ill, National Association of Anorexia Nervosa and Associated Disorders, National Association of County Behavioral Health Directors, National Association of Protection and Advocacy Systems, National Association of Psychiatric Treatment Centers for Children, National Association of Rural Mental Health, National Association of School Psychologists, National Association of Social Workers, National Council for Community Behavioral Healthcare, National Depressive and Manic-Depressive Association, National Foundation for Depressive Illness, National Mental Health Association, Tourette Syndrome Association, National organizations representing consumers, family members, advocates, professionals and providers.

PHARMACEUTICAL RESEARCH AND MANUFACTURERS OF AMERICA,
1100 FIFTEENTH ST. NW,
Washington, DC.
February 13, 2001.

The Honorable TOMMY G. THOMPSON,
Secretary, U.S. Department of Health and Human Services,
Hubert H. Humphrey Building,
200 Independence Avenue, SW,
Washington, DC.

DEAR SECRETARY THOMPSON: On behalf of the Pharmaceutical Research and Manufacturers of America (PhRMA), I am writing to ask that you take appropriate steps to delay the February 26, 2001 effective date for the "Standards for the Privacy of Individually Identifiable Health Information" to allow the Department to consider revisions of certain aspects of this enormously complex and important final rule.

PhRMA is firmly committed to protecting the confidentiality of individually identifiable health information, and we have long supported the adoption of Federal standards that would provide nationally uniform confidentiality protections. We believe patients deserve to know that their personal health information is protected; they also deserve answers to unmet medical needs.

Virtually all research necessary to demonstrate and monitor the safety and effectiveness of new medicines depends on data from patients and their health care providers or health plans. In our comments on the Department's proposed privacy regulation, PhRMA and its member companies underscored the importance of protecting the public health interest in research as well as the patient's right to privacy. We also expressed concern about the chilling effect the proposed regulation would have on the willingness of providers and health plans to participate in research given the complex, burdensome, and costly compliance requirements they would face, the ambiguities contained in the proposed regulatory framework, and the substantial penalties even the most technical violations might trigger.

PhRMA recognizes that HHS has sought to address and balance the many comments it received on the proposed privacy regulation. While the final regulation has been improved over the proposed version with respect to research, we remain concerned that it does not strike an adequate balance between individual privacy and legitimate uses of personal health information for biomedical research, including product safety and effectiveness surveillance activities.

The final regulation will require comprehensive and substantial changes in the way informed consent is obtained for treatment and for research, and it modifies certain long-standing Common Rule requirements and procedures without evidence of any privacy abuses under the Common Rule. These changes could have serious unintended consequences by discouraging broad provider and health plan participation in research and by diminishing the availability of data for biomedical research and innovation. Further, the regulation's stringent authorization requirements are likely to impede retrospective and outcomes research, as well as post-marketing sur-

veillance initiatives and important epidemiological studies. These concerns are further described below.

Modification of Common Rule

In our comments on the proposed privacy regulation, PhRMA urged HHS to avoid imposing unnecessary and burdensome conditions on research studies by modifying the Common Rule, because the Common Rule already adequately protects the rights of research study subjects. Clinical research is required in order to demonstrate the safety and effectiveness of the medicines that answer unmet medical needs. This type of research is carried out at great expense by research-based pharmaceutical companies that sponsor large-scale clinical trials on new drugs or on existing drugs for new uses. The companies submit the results of clinical trials to the FDA, which determines whether the drugs have thereby been demonstrated to be safe and effective. These trials are governed by FDA regulations, which incorporate among other requirements the long-standing provisions of the Common Rule, a universally accepted set of principles and procedures that govern biomedical research involving the use of human subjects.

The Common Rule details the informed consent process and other practices to be employed in clinical trials to appropriately protect the interests of the study subjects. Within this extensive and well-established regulatory framework, sponsors of studies have long engaged medical centers to conduct clinical studies of innovative pharmaceutical products. Over time, the sponsors and the study sites, with the oversight of Institutional Review Boards (IRBs), have developed procedures and processes to accommodate the objectives of the research in an efficient way, while also meeting the Common Rule requirements specifically designed to protect the rights and welfare of the human subjects.

Given the extensive protections and regulatory oversight necessarily present in Common Rule research, it is not surprising that there has been an absence of abuse of the privacy rights of study subjects of the kind the new privacy regulation seeks to remedy. The drafters of the regulation do not cite in their extensive preamble, nor are we aware of, claims that participation in clinical trials has given rise to the type of privacy concerns that have been widely reported in less regulated areas.

The final regulation, however, modifies the Common Rule in several consequential ways: first, by significantly expanding the scope of non-interventional (records-based) research that will now be subject to IRB review; second, by greatly increasing the administrative complexity and cost of implementing stringent new authorization, consent, notice, and tracking requirements that research institutions and other covered entities will have to assume; and, third, by introducing several new and, in some instances, highly subjective criteria for the waiver of authorization that IRBs and privacy boards will be required to apply. The combined impact of these changes threaten to impose important constraints on biomedical and other forms of research.

The final privacy rule has been clarified such that the authorization required or waived under the privacy regulation is entirely independent of the informed consent obtained or waived under the Common Rule. In effect, two entirely separate assents are now required of each research participant: (1) informed consent to participate in research under the Common Rule, and (2) "authorization" for certain medical information to be disclosed and used for research under the privacy rule. Although an IRB can waive either or both forms of individual assent, it must make a finding with respect to both. Moreover, any research that does not use a form that includes the extremely detailed authorization requirements established by the regulation must have a specific waiver of the form of authorization by the IRB or a privacy board.

These changes are likely to tax significantly the resources and capacity of most IRBs. They also will increase the administrative costs and complexities which covered entities (hospitals, doctors, health plans) must manage in obtaining required consents and authorizations (or waivers), meeting required tracking and notification requirements for all disclosures of protected health information, and ensuring that new privacy rights are appropriately administered. Given the enormous quantity of health research that requires access to archived patient records, compliance with the final regulation will put a particularly heavy administrative and financial burden on research institutions, particularly, academic medical centers and hospitals. This could lead to a diminution of the critical resources and support they are prepared to commit to research activities.

From a patient perspective, the highly prescriptive and bureaucratic process for authorization for disclosure and use of personal health information for research also will create the need for extensive patient explanation and discussion on the part of providers involved in clinical research, with a sponsor or otherwise. The sheer com-

plexity of the procedural requirements involved and the mortgage document-like character of the various assent forms that potential research subjects will be confronted with raise legitimate concern about whether patients (and their physicians) will be less willing, rather than more willing, to participate in research under the new privacy protection regime.

Criteria for Waiving Patient Authorization

Several new criteria for waiver of patient authorization of disclosure and use of protected health information for research have been added to those previously used by IRBs under the Common Rule's requirements. The highly subjective nature of some of these criteria raises concern about how they can reasonably be applied. For example, IRBs and privacy boards will be required to make determinations as to whether the privacy risks to individuals are "reasonable in relation to the anticipated benefits, if any, to the individuals, and the importance of the knowledge to be obtained from that research." Another criterion requires a determination of whether "the alteration or waiver will not adversely affect the privacy rights and the welfare" of the individuals involved. Inconsistencies in the way such criteria may be interpreted and applied could seriously compromise certain kinds of research that depend on access to protected health information from multiple IRBs or privacy boards.

De-identification

The final rule retains important impediments to the creation and use of deidentified data that will be suitable for research. The presumptive "safe harbor" method prescribed by the regulation makes more explicit the list of 18 "identifiers" that must be removed for the safe harbor to apply. At the same time, this method is even more obviously inappropriate for creating data sets that will be useful for many types of research, especially for outcomes and epidemiological studies. This is because it requires the deletion of facts that are essential for many health analyses, such as birth dates, hospital admission and discharge dates, individual zip codes, and unique medical conditions.

The alternative method recognized by the regulation essentially relies on the use of a statistician to create a database that, with appropriate coding or encryption, can be demonstrated to be effectively de-identified, whether used alone or in combination with other available information. However, it remains unclear whether, in practice, this approach will be too burdensome or costly to be applied for producing databases suitable for scientifically valid studies for most types of clinical, outcomes or epidemiological research.

Patient Exposure Registries and Adverse Event Reporting

Our public health system depends on a host of surveillance and reporting activities that take place under state and federal law, as well as the ethical responsibilities voluntarily assumed by health care providers, individuals and corporations. Patient exposure registries are one such activity that pharmaceutical manufacturers undertake to gather valuable safety and effectiveness information about far more diverse patient populations and varying conditions than can be studied under clinical trials designed to meet FDA requirements for product approval. For example, patient registries may be established to determine the relative frequency of problems, if any, experienced by patients taking a product during pregnancy, or products taken in combination with another product. The methodology relies on collecting a suitable sample of exposures and querying providers regarding any side effects, compliance issues or adverse events. Such feedback and information are important to provision of ongoing innovation, as well as to quality health care.

The final rule, however, specifically and unnecessarily limits "patient registries" to those that are created as "required or directed" by FDA. Otherwise, patient authorization in the form prescribed by the regulation, or waiver of authorization by an IRB or privacy board, is required as discussed above. Because FDA may regard its authority to "direct" manufacturers to create registries to be limited to certain fast-track approvals, manufacturers will be faced with the need to convince each physician who may report cases that she or he will not face legal sanctions for reporting case-specific information to the registry.

With respect to adverse event reporting, the new language of the regulation—a person "required or directed" by FDA—is clear but not helpful, since the average physician has little way of knowing which manufacturer has been required or directed to report adverse events. For some products, moreover, the manufacturer's role in collecting information about adverse events may not involve contacting or questioning covered entities pursuant to specific requirements or direction from the FDA or some other public health authority. For example, a manufacturer may establish a hotline for providers to spontaneously make these adverse event reports, and ensure that the hotline is available with product labeling. Here, too, provider uncertainty about possible liability exposure could impede the timely flow of impor-

tant information about adverse events and unreasonably compromise the viability of these important surveillance activities.

Mr. Secretary, the final privacy regulation has significant implications for the future balance between individual privacy and the public health interest in research and medical innovation. As many other organizations have pointed out, the regulation contains substantive changes from the proposed regulation, including entirely new sections and requirements that were neither in the proposed regulation nor foreseeable by those commenting on the proposed regulation. This fact alone argues for a new public comment period.

PhRMA requests that you take steps necessary to delay the February 26, 2001 effective date of the regulation to give the Department an adequate opportunity to review the areas of concerns we and other health care organizations have raised. PhRMA and its member companies are eager to work with you to develop effective protections for the privacy of individuals while safeguarding the public interest in medical innovations and efficiencies made possible by research.

Sincerely,

ALAN F. HOLMER

PREPARED STATEMENT OF THE NATIONAL ASSOCIATION OF CHAIN DRUG STORES

Mr. Chairman and Members of the Committee. The National Association of Chain Drug Stores (NACDS) appreciates the opportunity to submit comments to the Committee for this critical hearing on the impact on patients and providers of the regulations recently issued by the Department of Health and Human Services to protect the privacy of individually-identifiable health information.

The National Association of Chain Drug Stores (NACDS) membership consists of nearly 170 retail chain community pharmacy companies. Collectively, chain community pharmacy comprises the largest component of pharmacy practice with over 94,000 pharmacists. The chain community pharmacy industry is comprised of more than 20,000 traditional chain drug stores, 7,800 supermarket pharmacies and 5,300 mass merchant pharmacies. The NACDS membership base operates over 33,000 retail community pharmacies with annual sales totaling over \$400 billion, including \$160 billion in sales for prescription drugs and over-the-counter (OTC) medications. Chain operated community retail pharmacies fill over 60 percent of 3 billion prescriptions dispensed annually in the United States.

Community Retail Pharmacies Protect Patient Information

The community retail pharmacy industry is committed to safeguarding the privacy of patient medical records. Currently, in most states, licensed pharmacists must abide by patient privacy standards specified in state pharmacy practice acts, state board of pharmacy regulations, and other state laws. In addition to these requirements, retail pharmacies commonly require employees to comply with stringent patient privacy policies.

We have always believed that any new Federal privacy standards that are developed, whether through statute or regulation, must strike the appropriate balance of assuring that any new protections do not outweigh the ability of patients to obtain prescription services in a timely and efficient manner.

We believe that the final regulation does make some improvements over requirements in the proposed rule. Unfortunately, while we are still analyzing the impact of the final regulations on community pharmacies, we believe that these new regulations, if implemented in their current form, are unworkable and will have unintended consequences for community retail pharmacies and the patients that we serve.

Our industry is committed to providing prescription services as efficiently as possible, keeping in mind that our goal is to also help patients make the best use of their medications through education and counseling. We are meeting these objectives in an era of unprecedented demand for prescription services. Community pharmacies are filling more prescriptions than ever. In 2000, we filled an estimated 3.1 billion prescriptions. That number is expected to increase to 4 billion by 2004—just three years away. To keep pace with the demand for these services, our pharmacies have incorporated several efficiencies into their operations. These efficiencies help fill prescriptions faster, freeing up the pharmacist to spend more time with patients.

We have also been meeting this increasing demand for prescription services in the wake of a critical national shortage of pharmacists, documented by the recent Congressionally requested study by the Health Resources and Services Administration (HRSA). This shortage has already resulted in some pharmacies in some regions of the country reducing their operating hours. This study, as well as other private sector studies, makes the case that more efficiencies are needed in pharmacies to meet the challenge of providing more prescription services.

However, the administrative burdens imposed on patients and pharmacies by these new privacy regulations could significantly erode the strides in efficiencies that have been made over the last decade in providing prescription services. As a result, we do not believe that these regulations strike the important balance of providing additional meaningful protections for patient information with the increasing need to efficiently provide pharmacy services. **New Pharmacy Prior Consent Requirements for Treatment, Payment and Operations**

Operations

NACDS supported the "statutory authorization" concept in the proposed rule. That is, we believe that the presentation by the patient (or their representative) to the pharmacist of a legally-valid prescription provides the necessary implied consent for the pharmacist to engage in the activities permitted by state law to fill the prescription within the boundaries specified by third-party prescription coverage plans, such as formulary management, and to provide the related professional services to the patient, such as refill reminders and information about treatment alternatives. This is, if the patient didn't want the prescription filled, he or she would not be bringing it to the pharmacy.

Moreover, we also believe that the prescription represents more than just providing a bottle of tablets or tube of cream to the patient. It represents the physician's intent for the patient to complete a course of prescription treatment as effectively as possible, for which the pharmacist has a continuing and expanding role.

However, among the most problematic aspects of the final rule is the new requirement, which was not in the proposed rule, that pharmacies, who are classified as "direct treatment providers," must obtain a written, signed consent from patients to being able to use or disclose individually-identifiable information for treatment, payment, or health care operations.

That is, pharmacies cannot fill or even begin the process of filling prescriptions before the patient's (or guardian's) signed, written consent is on file. More surprising to us is that even HHS said that such a prior consent requirement was unworkable, and rejected its use in the proposed rule. Yet, it was included in the final rule, without any opportunity for public comment. We do not believe that the full implications and unintended consequences of this written prior consent requirement are yet understood by patients.

For example, we believe that the new signed, written consent requirement will have the following impact on patient care and prescription services:

New and Refill Prescriptions: The need for the patient to provide a prior written consent means that pharmacists may not be able to fill or refill prescriptions for patients, and prescriptions called in by physicians may not be filled until that consent is on file at the pharmacy. This requirement will create delays for patients, for parents with sick children, and others, such as elderly and disabled individuals, who will have to come to the pharmacy to sign a consent or to send someone on their behalf to do so, before the pharmacist may fill or refill a prescription. While this would be highly impractical, we also have questions about whether the regulation requires a patient to actually sign the consent in the pharmacy's physical location, or if a representative of the patient can present the written, signed consent. With billions of prescriptions filled each year in the United States, disruptions in even a small percentage of these transactions could adversely impact millions of patients.

Senior "Snow Birds": Many seniors travel to other destinations in the winter (or summer). For all practical purposes, these seniors will have to sign another written consent for the pharmacy provider in their other destination in order for them to have their prescriptions filled. This would likely be the case even if they use the same chain pharmacy in the winter and summer locations, assuming that the chain has a "shared", chain-wide prescription processing system that can make note of consents that are already on file. This is because different states with different privacy laws will likely require the patient to sign another written consent at the pharmacy they use in the other state, even if part of the same chain.

Transferring Prescriptions: As is often the case, a patient may want to transfer their prescription from the pharmacy where it was filled originally to another pharmacy location to have it filled there. The patient may want to do this either because of a move, a preference for the other pharmacy, or because they want to pick it up after work from a closer pharmacy. If the pharmacy with the prescription and signed written consent on file transfers a prescription to another pharmacy that does not have the patient's signed written consent on file, or to an affiliated pharmacy within the same chain that is located in another state, then the patient will have to provide another written consent to the pharmacy to which the prescription is being transferred before the pharmacy can use the information to fill the prescrip-

tion. This will make it more difficult for the patient to pick up the prescription quickly.

Living and Working in Different States: A patient may live in one state, such as Virginia, but may want to fill a prescription where they work in the District of Columbia or Maryland. Even if they have a consent on file in a pharmacy location where they live, they will likely have to sign another consent in the pharmacy location where they work because the written consent is a recognition that the patient has read and understands their "privacy rights" in the state in which the service is being delivered. Without Federal preemption of state privacy laws, those rights will likely vary by state.

Transition Provisions: A pharmacy cannot use patient information that is already on file after the compliance date, February 26, 2003, without a signed, written consent. As a result, patients will find it more difficult to refill prescriptions until they come in with a signed, written consent form. To mitigate the impact of this requirement on patients, a pharmacy would theoretically have to contact every patient in its database before the compliance date, which could be literally tens of millions of individuals, and have them mail or fax back a written consent, or the patient would have to come in and provide a signed written consent.

The impact of this requirement on public health is significant. For the pharmacy to continue to perform quality assurance, outcomes evaluations, send refill reminders, perform drug utilization review (DUR), and other functions with the information already in the system, the pharmacy has to obtain written consents before February 26, 2003 for every active patient in the database. The final rule also sharply underestimates the cost to providers of executing this step, and contacting and obtaining consent from each and every patient.

Prescription Noncompliance: After the regulation's compliance date, patients that are noncompliant with chronic-use medications, and that rely on refill reminder letters from their pharmacist, would not be able to receive these reminder letters unless the pharmacist had a signed, written consent on file. Noncompliance with prescription medication is already a significant public health problem contributing to additional morbidity, mortality and costs to the health care system. This is especially the case for patients with high blood pressure, high cholesterol, and diabetes. If pharmacists are unable to contact their patients already in their system about their prescription refills after the regulatory compliance date, the implications of prescription noncompliance will only worsen.

Rejected Prescription Claims: Prescription claims that were filed before the compliance date, but were rejected by a insurance company, PBM, or third party payor after the compliance date could not be resubmitted by the pharmacy for payment until the pharmacist can obtain consent from the patient to bill the third party claimant. Many of these prescription claims are rejected for simple omission of basic information on the prescription claim, but are easily corrected and resubmitted for payment. However, if pharmacies are unable to contact the patients whose prescription claims were rejected, and submit these claims, it could result in significant loss in business revenue for pharmacies. This is a serious issue for pharmacies, given about 85 percent of all prescriptions are paid for by third-party plans.

Impact on Prescription Costs: We are concerned that the proposed rules may limit the ability of private and public health care plans to manage their pharmaceutical expenditures. For example, while the regulations allow for drug formulary management as part of "health care operations", the definitions of "marketing", "treatment", and "health care operations" overlap in many places and are unclear. Some formulary activities could fall under each of the various definitions. If the health care system has any hope of better managing pharmaceutical expenditures, especially with a new Medicare prescription drug benefit, then the private and public sectors must have the ability to develop and manage drug formularies effectively, and provide options for lower-cost therapeutic alternates.

These are among the many examples that we have identified regarding the impact that this new written consent requirement will have on pharmacy providers and the patients that we serve. Unfortunately, in low-margin, high-volume community pharmacies, new requirements that add administrative burdens to the system will invariably result in delays for patients and additional costs to the system. We question whether the benefits of this new consent requirement will really outweigh the costs to the system, and the potential unintended consequences on patient care.

Federal Pre-Emption of State-Based Privacy Laws

NACIDS believes that new comprehensive federal standards should preempt state privacy laws. Community retail pharmacies, operating thousands of chain pharmacies in multiple states, need one federal standard rather than 50 different standards to interpret. Subsequently, conflicts between federal and state law could be virtually impossible for health care providers to resolve on a patient-by-patient basis.

This final regulation does not pre-empt many state-based privacy laws. In fact, states can and likely will enact stronger privacy laws, creating a situation where providers will have to determine themselves which is stronger—state based laws, Federal regulations, or court cases relating to patient privacy that might be relevant in particular situations. Moreover, the final rule does not provide for the Secretary to issue guidance to providers concerning which state laws are contrary to and more restrictive than the rule or to regularly update the guidance.

As a result, community pharmacies will have to develop a process to regularly monitor which law, regulation, or court case should be applied, and have to update their "privacy notices" accordingly. Given the significant length and scope of the privacy notices and consents required under the rule, the cost of changing and re-issuing them every time a state law or regulation is changed is staggering. This is especially true when you are providing billions of prescriptions each year, and are operating in multiple states.

While we understand that only a new Federal statute can pre-empt state law, not Federal regulations, we believe that Federal policy makers should take action this year to pre-empt state laws and create nationally uniform Federal privacy protections.

Conclusion

NACDS and its member companies want to reiterate our commitment to strong, Federal standards—with state preemption—to protect the privacy of medical records. We are seriously concerned about this new written prior consent requirement in the final HHS regulations for direct treatment providers, which did not appear in the proposed rule, and for which public comment has not been allowed or the implications for patients adequately assessed.

We believe that this new written prior consent requirement, especially for the billions of prescriptions filled annually by community retail pharmacies, presents significant operational, logistical, and patient care challenges, and that the unintended consequences of this requirement will result in patient frustration and longer waiting times at the pharmacy counter.

We have joined with other organizations in asking Secretary Thompson to delay the February 26, 2001 effective date of the rule and to work with us, as well as other affected parties, to determine how we might best address these and other important implementation issues. We want to work with Members of this Committee and the Congress to assure that reasonable privacy protections result from this process, and that patients' access to efficient, effective pharmacy services remains. Please contact us with any questions about this testimony. Thank you for the opportunity to submit these comments for the record.

PREPARED STATEMENT OF THE AMERICAN PSYCHOANALYTICAL ASSOCIATION

The American Psychoanalytic Association (the "American") submits the following testimony to be included in the record of the above hearing held before the Senate Health, Education, Labor and Pensions Committee on February 8, 2001. The "American" was established in 1911 and is one of the oldest mental health associations country. It has approximately 3500 members who are engaged in both private clinical practice and in research. Members of the "American" have affiliations with many of the most prominent academic medical institutions in the country.

I. Response to the question presented—the short answer

This hearing was convened to address the following question: Does the final HHS medical information privacy regulation make patient privacy a reality? The American believes that the regulation does not fully or completely achieve that objective but that it takes a significant step that is essential to preserving access to quality health care.

The American further believes that, in view of the importance of medical privacy to quality health care, the implementation of this regulation should not be further delayed. In any event, none of the other provisions of HIPAA which facilitate the transmission and compilation of identifiable health information should be put into effect until the privacy protections of this regulation have been fully implemented.

The American believes that improvements are needed in the regulation before it can be said that medical privacy is a reality in all appropriate circumstances. The Department of Health and Human Services, however, has expressed a willingness to refine the regulation through interpretations and amendment, and the American believes that this process should be given a chance to work before any consideration is given to disrupting the implementation timetable of the regulation.

The rulemaking record contains extensive evidence showing that protecting the privacy of identifiable health information, and particularly identifiable mental health information, is essential to preserving access to quality health care. 65 Fed.

Reg. at 82464-469; 82472-474; 82514. The record also is replete with survey evidence that the protection of medical information privacy is essential for the public to retain trust and confidence in the health delivery system and that this trust and confidence is increasingly being eroded by developments in technology that dramatically increase the ability of entities to compile and disseminate identifiable health information and to obtain and use genetic as well as other identifiable health information. 65 Fed. Reg. at 82465466.

Based on this uncontradicted evidence in the rulemaking record, the American believes that any further delay in the implementation of the medical information privacy regulation will result in a further loss of public trust in the health delivery system and a loss of access to quality health care. More specifically, it is now beyond dispute that the failure to provide strict privacy protection for communications between a psychotherapist and a patient will eliminate access to effective psychotherapy. See findings to this effect in *Jaffee v. Redmond*, 116 S.Ct. 1923 (1996) and *Mental Health: A Report of the Surgeon General*, 449 (December 1999). While improvements are needed, the American believes that the special protections which the regulation affords "psychotherapy notes", are essential for preserving access to effective psychotherapy. 45 CFR sec. 164.508(a)(2).

I. Comments on Issues Raised at the Hearing

At the hearing, the General Accounting Office summarized some of the issues and concerns raised by certain interested groups. See *Regulation Enhances Protection of Patient Records but Raises Practical Concerns*, Statement of Leslie G. Aronovitz, Director Health Care-Program Administration and Integrity Issues. The American believes that there is additional information that it is important for the Committee to take into account in considering the testimony of GAO and others.

A. GAO finds that HHS was responsive to comments

The GAO testimony notes that when it reviewed the comments on the proposed privacy regulation, there were "two overriding themes": (1) "a widespread acknowledgement of the importance of protecting the privacy of medical records" and (2) "the conflicts that arise in attempts to balance protecting patients' privacy and permitting the flow of health information for necessary uses". According to GAO, "most groups . . . acknowledged that HHS was responsive in addressing many of their comments on the draft regulation".

The American generally agrees with GAO's findings, but believes that HHS erred in failing to prioritize the inflicting interests. The record shows that an essential element of quality health care is the justifiable expectation by the patient that disclosures to a practitioner will not be further used or disclosed without the patient's permission. Based on this finding, the Supreme Court in *Jaffee v. Redmond* expressly rejected a "balancing" test for the protection of psychotherapy communications on the grounds that patients "must be able to predict with some degree of certainty whether particular discussions will be protected". 116 S. Ct. at 1932. (The Court had previously noted that there was no conflict between the interests of the public and the interests of the individual since access to effective psychotherapy was in both the public as well as the private interest. 116 S. Ct. at 1929.)

Accordingly, the American believes that protecting the privacy of identifiable health information, and particularly psychotherapy communications, should be given the highest priority and that other national "priorities" should be considered only to the extent that they can be achieved while preserving the patient's right to privacy for his or her identifiable health information.

A. Consent and disclosure provisions attract a range of concerns

We agree with the position of several of the consumer and practitioner associations surveyed that the regulation's requirements for consent and/or authorization for many disclosures was "a step forward in the protection of personal health information". We share the concern raised by some that regulation's permissive use of protected health information for marketing without authorization runs in conflict with underlying regulatory scheme. 164.514(e).

The most glaring example of this inconsistency is that the regulations require a patient's own physician to obtain consent before using or disclosing protected health information to treat the patient (164-506). Any covered entity is permitted to use or disclose the patient's protected health information for marketing without consent or authorization. Surveys show that patients are less concerned about disclosing information to their practitioners for use in their own care but are increasingly concerned that their identifiable health information will be used without their consent for marketing. As the preamble to the proposed rule correctly noted, "... individuals probably do not envision that the information they provide when getting health care would be disclosed for such unrelated purposes [such as marketing]". 64 Fed. Reg. at 59952.

HHS told GAO that patients could restrict the use of their protected information for such purposes. But, as GAO pointed out, providers are not required to agree to such requests.

A. Some stakeholders raised concerns about costs and feasibility

GAO noted that some stakeholders, principally a hospital association and a health insurer, raised concerns about the feasibility of implementing compliance measures by the compliance dates and about the compliance costs. We believe that those concerns are premature and overstated.

First, it is important to note that the compliance dates were more than two years beyond the December 28, 2000 publication date of the final regulation.

Second, the compliance date for providers (February 26, 2003) is a "soft", rather than a "hard" compliance date. The regulation provides for a transition period beginning on the compliance date under which providers may continue to use and disclose protected health information pursuant to "a consent, authorization, or other express legal permission" obtained prior to the compliance date even if those expressions of permission do not comply with the regulation. 164.532. So, the regulation will be phased into effect beginning with new patients accepted after the compliance date in 2003.

Third, the regulations have already been delayed beyond the deadline set forth in the statute. Section 264 of HIPAA required the regulations to be issued 69not later than" February 21, 2000. The regulations were issued more than 10 months beyond the statutory deadline (after the deadline for comments had been extended), and the effective date is more than a year after that deadline. The compliance date is more than three years after the statutory deadline. It is simply not in the public's interest to provide a further delay in a regulation that contains the standards for protecting the public's right to privacy and right to access for identifiable health information. With the kind of lead time which has already been provided, it is likely that some organizations will contend that even a further extension will not provide adequate time for compliance.

Fourth, it is difficult to imagine that providers, and particularly hospitals, will experience exorbitant costs in implementing the requirements of the regulation if they have been complying with privacy requirements already in effect under Medicare conditions of participation and standards issued by the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO). Under Medicare, hospitals are required to "protect and promote" the right of patients to personal privacy. 42 CFR sec. 482.13 and 482.24(b)(3). JCAHO standards contain detailed requirements for hospitals to respect patient needs for confidentiality and privacy. JCAHO Standards RI. 1.3.

Whatever the cost to providers of protecting patients' rights to medical privacy, it is likely to be outweighed by the patients' reluctance to seek needed health care and make disclosures necessary for accurate diagnosis and treatment which would be the inevitable result of failing to protect the privacy of identifiable health information.

Further, the protection of medical information privacy is necessary to further the underlying statutory objective. Section 261 of HIPAA states that the intent of the act was to "improve ... the efficiency and effectiveness of the health care system". As studies have shown consistently (and the Supreme Court has noted with respect to psychotherapy communications), the health care system cannot operate effectively unless patients have trust and confidence that their personal health information will not be used or disclosed without their consent or authorization.

A. Views were divided on partial preemption of state laws

According to GAO, consumers and practitioners supported the preservation of state privacy laws that provide greater privacy protection while groups representing insurers and employers considered the partial preemption ii operationally cumbersome". As GAO noted, "every state has passed legislation to protect medical privacy". Some of the laws are more comprehensive than others.

Congress should be reluctant to preempt an area where every state has acted. This regulation adopts the moderate approach that was required by section 11 78(a)(2)(B) of the Social Security Act and establishes a "new federal floor of privacy protections that does not disturb more protective rules or practices." 65 Fed. Reg. at 82471. This is an approach that is consistent with the Administration's view of the federal government's role in areas such as education.

State laws that afford greater privacy protection should not be preempted in the interest of convenience of multi-state insurers and employers. These insurers and employers presumably have already assessed the business risk of operating in more than one state and have arranged their affairs to accommodate that "complexity". By establishing a uniform federal floor of privacy protection, this regulation should

significantly simplify, rather than complicate, the requirements that multistate organizations have had to meet in the past.

I. Suggestions for improvements in the final regulation

As stated, we believe that implementation of the regulation should not be delayed further and that improvements and clarification should be implemented through interpretative guidelines and amendments where necessary. Some of the improvements and clarifications we suggest are as follows:

A. The exclusions from the special protections afforded psychotherapy notes should be interpreted in such a manner that the special protections encompass the information that would be included in the therapist-patient privilege recognized in *Jaffee v. Redmond*.

B. It should be made clear that a psychotherapist should not be coerced into including privileged communications in the patient's general medical record as a condition of participating in a health insurance plan.

C. Protected health information should not be used or disclosed for marketing without the patient's authorization.

D. Protected health information should not be used or disclosed without the patient's consent or authorization in response to an administrative request unless there has been a determination by an independent individual that there is probable cause to believe a law has been violated.

In summary, we believe that the final health information privacy regulation, while in need of improvement, represents a laudable effort to address a difficult issue and is essential to preserving access to quality health care for all Americans.

PREPARED STATEMENT OF THE HEALTHCARE LEADERSHIP COUNCIL

Mr. Chairman and members of the Committee, the Healthcare Leadership Council (HLC) appreciates this opportunity to submit testimony to the Committee for this important hearing on the final HHS Privacy Regulations. The HLC is an organization of chief executives of the nation's leading health care companies and institutions. The HLC also founded and currently chairs the 120-member Confidentiality Coalition.

The establishment of uniform federal standards for the protection of patient information has long been our goal. In judging regulatory or legislative proposals on medical confidentiality, our overriding consideration is what is ultimately best for the patient. The HLC believes that balancing the goals of protecting confidentiality and allowing the free flow of medical information for high quality patient care is achievable. The importance of getting this balance right cannot be overstated. Patient information is the lifeblood of quality health care. Virtually every health hazard we know of today—from AIDS, to smoking, to polio, to measles - has been identified using medical records. Every advance in the delivery of health care has been developed using medical records.

As mentioned, the HLC and the larger Confidentiality Coalition have spent countless hours since the final HHS regulation was published in December poring over this extremely complex rule. While we now have a good working knowledge of the rule, it may take additional weeks or months for us to uncover potential problems. By the end of February, HLC will be submitting to Congress and the administration a detailed list of concerns, questions, and areas needing clarification. However, we have reached several important conclusions:

In some regards, the final rule is an improvement over the proposed version and addresses some of the concerns about which we commented. While clarification is needed on dozens of points, the "business partner" section is better, the research section is improved, an attempt was made to improve the "minimum necessary" section (but problems remain), and the potential for a private right of action was lessened (but not removed).

Key new provisions have been added to the final regulation that are unworkable and could seriously disrupt patient care. We are especially concerned about the impact of the new provision that requires that providers obtain the prior specific written consent to use or disclose identifiable information for treatment, payment, and health care operations. There was no opportunity for groups to comment on this major new provision because it was not in the proposed regulations and, in fact, HHS took great pains to explain why such a consent scheme was unworkable and therefore not included.

While an attempt was made to fix aspects of the proposed rule, several provisions need clarification so as not to disrupt quality patient care. For example, clarification is needed as to whether the rule requires hospitals, clinics, and other covered entities to limit information to the "minimum necessary" when treating patients.

The lack of adequate transition provisions in the rule raise the possibility of severe disruptions in the delivery of health care to patients and consumers two years from now.

Problems remain with the final regulation with respect to research that could impose significant new burdens and record-keeping requirements on research institutions that will divert resources from research.

Finally, the regulation's cost of compliance runs contrary to the Health Insurance Portability and Accountability Act (HIPAA) requirement that the privacy standards reduce the administrative costs of providing health care.

For these reasons, the HLC and 40 other groups representing the health care delivery system (see attached letter to HHS) are calling on the administration to delay the February 26 effective date of the regulation to give them an opportunity to address these concerns.

Aspects of the Final Rule that Are Improved

The final rule appears to allow the use of population data to support patient treatment and other healthcare activities. The use of this data is important to allow health plans, hospitals, and others to review entire enrollee and patient databases to identify individuals whose utilization patterns of asthma drugs, or emergency room visits, for instance, indicate they would benefit from disease management programs.

The final rule has clarified and more appropriately limited the responsibility that covered entities have for "business partners." While the rule does not need to regulate business partners at all to protect confidentiality, the rule is improved in this respect nevertheless. There remain points of clarification needed with some aspects of what the rule now calls "business associates."

There are improvements in the final rule with respect to de-identifying patient information. The final rule provides an alternative process for de-identifying patient information that allows information to be deemed de-identified by using "generally accepted statistical . . . methods" and determining that there is a very small risk that the individual could be identified.

As mentioned, there are also improvements in the research provisions of the regulation.

Key Areas of Concern

The HLC is especially concerned about the impact of the new provision that requires that patients sign a specific patient consent before providers may use or disclose identifiable information for treatment, payment, or health care operations. This provision was not part of the proposed regulation. In fact, the proposed regulation took an entirely different approach which we strongly supported, the "statutory authorization."

HHS, in the proposed regulation, went to great lengths to explain why a consent requirement was unworkable and therefore rejected. The state of Maine repealed a similar requirement in 1999 just 12 days after it took effect due to severe disruptions for family members trying to obtain prescriptions for elderly parents and other family members.

This provision will have its most serious consequences (but not the only consequences) for millions of patients and health professionals attempting to order, fill, refill, and pick up prescriptions. In 2000, pharmacies filled an estimated 3.1 billion prescriptions in the United States, a figure projected to rise to 4 billion by 2004.

This new requirement will prohibit pharmacies from filling prescriptions before the patient's signed, written consent is on file—a consent that is not now obtained. When this provision is enforced in February 2003, the problems will arise for new and refill prescriptions, prescriptions for senior "snow birds," prescriptions that are transferred to a new pharmacy, prescriptions for people living and working in different states, and prescriptions for which a claim was rejected and had to be refilled, and the many prescriptions picked up by relatives and friends.

The enormous rising volume of prescriptions combined with the fact that pharmacies and pharmacists do not currently obtain consent in filling a prescription, is a prescription for serious disruption for millions and millions of patients. Add to this potent mix the extreme shortage of pharmacists, and the problem is considerably worse.

The problems created by this new consent requirement will also extend to other health care providers including doctors, dentists, hospitals, and others.

The lack of adequate transition rules for the consent requirement creates the potential for serious disruptions, as well. As of February 2001, no health care provider will be able to use or disclose patient information for treatment, payment, or health care operations without a signed consent form on file. That consent form must, apparently, require that permission was given for the "use or disclosure" of information for "treatment, payment and health care operations." Many consent forms com-

monly used in doctors' offices and hospitals dealing with patient information are limited to disclosure of information for payment of claims activities. They are often not permitted to "use" information for treatment or health care operations activities. This raises an important question as to whether providers can use information for ongoing treatment and health care operation activities, such as reminder notices about appointments, conducting disease management programs, maintaining quality assurance programs, and so on, will be possible.

As mentioned, because pharmacies do not currently obtain any consents whatsoever for use or disclosure (nor are they required to by most state laws), they would clearly be unable to fill or refill prescriptions as of February 2003 until the individual delivers a signed consent form.

The final regulation needs clarification as to whether it requires covered entities to limit information to the "minimum necessary" when using patient information for treatment. The rule excludes "disclosures to or requests by" a health care provider for treatment from the "minimum necessary" rule, but is less clear on whether the standard applies to "use" of information. This is not a minor technical detail. Definitive clarification is needed that use of patient information for treatment is not subject to the minimum necessary rule. Limiting the ability of teams of health professionals, and health profession trainees, in a hospital setting to use a patient's complete medical chart or freely discuss and communicate among themselves in the course of treating patients could be disruptive and potentially dangerous.

The notice requirements of the rule will require potentially pages and pages of information about how information will be used and disclosed. This lengthy form will have to be made available to every consumer, every patient, before consent for treatment, payment, and health care operations may be obtained. The form will have to be changed and reprinted with every change in the way information is used and disclosed. The costs and burdens on providers of printing, maintaining, and disseminating these notices to every patient will be enormous. Also, the complexity and sheer volume of these notices are such that the value to patients—like so many forms signed at a mortgage closing—may become less useful and meaningful.

By modifying the Common Rule with respect to the enormous quantity of health research that requires access to archived patient records, the final regulation will impose significant new burdens and record-keeping requirements on research institutions that will divert resources from research. In addition, we are concerned about the new requirement that Institutional Review Boards (IRBs) make determinations as to whether the privacy risks to individuals are "reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge to be obtained from that research." This introduces into the IRB process a determination for which there are no normative standards, and which will of necessity be based on the belief structures and ideologies of individual IRB members.

The final regulation appears to be contrary to HIPAA's goal and requirement that the privacy standards reduce the administrative costs of health care. HHS estimates that the privacy rule will increase the cost of providing health care by \$18 billion.

This is by no means an exhaustive list of all of the concerns the HLC has identified. As mentioned, we plan to submit to Congress and the administration a more detailed and extensive list of areas that are of concern or need clarification.

We thank the committee for this opportunity to testify and look forward to working with you in the coming months to improve this regulation.

PREPARED STATEMENT OF THE ASSOCIATION FOR HEALTHCARE PHILANTHROPY,
WILLIAM C. MCGINLY, PH.D., CAE, PRESIDENT, CHIEF EXECUTIVE OFFICER

The Association for Healthcare Philanthropy (AHP) is pleased to present its comments for the written record on the HHS regulations concerning the standards for privacy of individually identifiable health information.

Established in 1967, the Association for Healthcare Philanthropy (AHP) is a not-for-profit organization whose 3,000 members manage philanthropic programs of foundations and development departments in 1,700 of the nation's 3,400 not-for-profit, charitable health care providers. Our members are professional development executives whose mission is to support local health care programs through philanthropic fund raising.

As AHP's president and chief executive officer, I can tell you that an estimated 75 percent to 80 percent of the U.S. population resides in the areas served by these providers, which include community hospitals and medical centers (59 percent), multihospital systems (14 percent), specialty institutions (8 percent), academic institutions (5 percent), long-term care facilities (5 percent), and other not-for-profit facilities (9 percent).

In 1999, AfIP's members elevated the level of health care services in the communities in which they work and live by raising \$6 billion. In FY1998, AHP's members raised more than \$5.7 billion—\$1.92 billion more than was raised by all of United Way of America during the same time period. The money raised helps fund, among others:

- wellness programs,
- mobile health vans,
- mammography screenings,
- hearing and eye exams,
- hospital facility improvements,
- essential upgrades,
- and health care services for the uninsured.

Such programs are central to the not-for-profit mission of AHP members' institutions and organizations. They are an integral part of their business. For such programs to continue, AHP's members must have access to their health care provider's database. The reason: More than 60% of funds raised each year come from individuals—most of whom are grateful patients.

The new HHS standards for protecting the privacy of Americans' personal health records recognize the critical role that philanthropic giving plays in the nonprofit health care provider community. As such, patient privacy is protected in the context of the fund raising that is done by the professional development executives who are responsible for the development departments of nonprofit health care providers.

While placing significant restrictions on the use of the patient's medical record and other personal health information, the regulations specifically permit a covered entity to engage in fund raising for its own benefit as part of "health care operations" without obtaining patient authorization. However, the covered entity is only allowed to utilize demographic information relating to an individual (i.e., name, address, gender, age) and dates of treatment to make charitable appeals. In addition, information on how an individual may opt out of future contacts must be provided.

Like all other entities impacted upon by the regulations, AHP's members and the nonprofit hospitals and foundations in which they work, are prohibited from using patient's medical information in their efforts. AHP wholeheartedly supports this limitation since in its 30+ years in existence, AfIP's members have utilized such information for the purpose of avoiding inappropriate contacts, such as with minors, the aged, and individuals with unresolved medical conditions.

In addition, when approaching prospective patient donors, AHP members are sworn to respect the confidentiality of patient information through the AHP Statement of Professional Standards and Conduct and its companion Bill of Donor Rights. Further, AHP members are committed to upholding the spirit and intent of state and federal laws governing use of patient information. The way in which AHP members' institutions and organizations handle confidential information might be likened to how colleges handle student records. That is, academic records are not released without authorization, even to tuition-paying parents, yet demographic data routinely is given to the alumni office for fund-raising efforts that ensure the support of the college's long-range educational mission.

Finally, the kind of marketing carried out by AfIP members is not the kind of marketing of commercial products that seems to be the real target of this regulation's restriction. It is important to remember the distinction between for-profit and not-for-profit ventures.

Nonprofit health care providers rely on philanthropic giving when budgeting to provide medical outreach in their communities. The HHS standards, with appropriate restrictions and requirements, allow these efforts to continue.

AHP Statement of Professional Standards and Conduct, Donor Bill of Rights, Letters from members follow:



Association for
Healthcare
Philanthropy

313 Park Avenue
Suite 400
Falls Church, Virginia 22046
(703) 532-6243
Fax (703) 532-7170

Association for Healthcare Philanthropy Statement of Professional Standards and Conduct

Association for Healthcare Philanthropy members represent to the public, by personal example and conduct, both their employer and their profession. They have, therefore, a duty to faithfully adhere to the highest standards and conduct in:

- I. Their promotion of the merits of their institutions and of excellence in health care generally, providing community leadership in cooperation with health, educational, cultural, and other organizations;
- II. Their words and actions, embodying respect for truth, honesty, fairness, free inquiry, and the opinions of others, treating all with equality and dignity;
- III. Their respect for all individuals without regard to race, color, sex, creed, ethnic or national identity, handicap, or age;
- IV. Their commitment to strive to increase professional and personal skills for improved service to their donors and institutions, to encourage and actively participate in career development for themselves and others whose roles include support for resource development functions, and to share freely their knowledge and experience with others as appropriate;
- V. Their continuing effort and energy to pursue new ideas and modifications to improve conditions for, and benefits to, donors and their institution;
- VI. Their avoidance of activities that might damage the reputation of any donor, their institution, any other resource development professional or the profession as a whole, or themselves, and to give full credit for the ideas, words, or images originated by others;
- VII. Their respect for the rights of privacy of others and the confidentiality of information gained in the pursuit of their professional duties;
- VIII. Their acceptance of a compensation method freely agreed upon and based on their institution's usual and customary compensation guidelines which have been established and approved for general institutional use while always remembering that: any compensation agreement should fully reflect the standards of professional conduct; and, antitrust laws in the United States prohibit limitation on compensation methods;
- IX. Their respect for the law and professional ethics as a standard of personal conduct, with full adherence to the policies and procedures of their institution;
- X. Their pledge to adhere to this Statement of Professional Standards and Conduct, and to encourage others to join them in observance of its guidelines.

A Donor Bill of Rights

Philanthropy is based on voluntary action for the common good. It is a tradition of giving and sharing that is primary to the quality of life. To assure that philanthropy merits the respect and trust of the general public, and that donors and prospective donors can have full confidence in the not-for-profit organizations and causes they are asked to support, we declare that all donors have these rights:

- I. To be informed of the organization's mission, of the way the organization intends to use donated resources, and of its capacity to use donations effectively for their intended purposes.
- II. To be informed of the identity of those serving on the organization's governing board, and to expect the board to exercise prudent judgment in its stewardship responsibilities.
- III. To have access to the organization's most recent financial statements.

- IV. To be assured their gifts will be used for the purposes for which they were given.
- V. To receive appropriate acknowledgment and recognition.
- VI. To be assured that information about their donations is handled with respect and with confidentiality to the extent provided by law.
- VII. To expect that all relationships with individuals representing organizations of interest to the donor will be professional in nature.
- VIII. To be informed whether those seeking donations are volunteers, employees of the organization or hired solicitors.
- IX. To have the opportunity for their names to be deleted from mailing lists that an organization may intend to share.
- X. To feel free to ask questions when making a donation and to receive prompt, truthful and forthright answers.

Developed by American Association of Fund Raising Counsel (AAFRC) Association for Healthcare Philanthropy (AHP) Council for Advancement and Support of Education (CASE) National Society of Fund Raising Executives (NSFRE). Endorsed by (in formation) Independent Sector National Catholic Development Conference (NCDC) National Committee on Planned Giving (NCPG) National Council for Resource Development (NCRD) United Way of America



JOHN MUIR FOUNDATION

A Charitable Organization of John Muir Medical Center

January 23, 2001

Mr. Bill McGinly
President, CEO
Association for Healthcare Philanthropy
313 Park Ave. Suite 400
Falls Church, VA. 22046

Dear Bill,

It was great to hear the news that we've had a favorable outcome regarding the privacy issues related to fundraising from our former and grateful patients. I'm not sure what the communication process is to inform new people at HHS about this issue. However, I'm sending this letter just in case you need a few specific reasons to explain the importance of access to patient demographic information for hospital foundations if the new Bush appointees need to be brought up to speed on the reasons behind the current regulation.

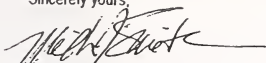
1. John Muir Medical Center Foundation raises money only for John Muir Medical Center and from time to time for programs shared by our sister medical center, Mt. Diablo.
2. Ours is an internal foundation, common among hospitals, and we therefore do not share our donor list with any other organization. Sharing lists is a common practice among large national fundraisers and fundraising organizations. The fact that we do not and have never shared lists is a most significant point and needs to be clearly understood by those at HHS.
3. We've been raising money from our grateful patients since the early 1960's. Because we protect and guard our donor information, and because we remove persons from our solicitation list at their first request, we have had almost no complaints about our process. In the six years I've been here we've had one, it was handled to the satisfaction of all.
4. As our medical centers continue to struggle with shrinking revenue and more demand for services, fundraising efforts are more important now than ever. In our case, not being allowed to solicit grateful patients could reduce our annual fundraising revenue by as much as \$1,000,000 per year. Long term losses could be even worse because so many of our major donors and deferred givers begin their giving as grateful patients. Some of the most popular services that could be effected are nursing education, medical equipment purchases, diabetes education, cancer care and other clinical and educational programs that are of interest to our community of 650,000.

5. In 2000 our two hospital system provided \$4 million (based on our cost) in charity care for our community. In 2001 we're budgeted to provide \$3.5million. As a 501(c)3 organization it is part of our mission to provide charity care as well as several million dollars worth of other community benefits. Any curtailment in our fundraising efforts make it just that much more difficult for us to achieve the mission our community has come to support and expect.

I hope this letter will be helpful as you and other AHP staff continue to work with those at HHS to ensure a healthy fund raising future for our country's many hospitals and medical centers. It is of utmost importance to our patients, our community, and to us.

Should you need any further help regarding this matter please feel free to call on me.

Sincerely yours,



Mitt J. Smith
President

MJS.mc

CARONDELET

FOUNDATION

January 30, 2001

A Part of

Carondelet
Health
Network

120 North
Tucson Blvd.

Tucson, AZ
85716-4740

(520) 319-5000

PO Box 13170

Tucson, AZ
85732-3170

Also part of
Carondelet.

St. Mary's
Hospital

St. Joseph's
Hospital

Holy Cross
Hospital

William C. McGinly, Ph.D., CAE
President, Chief Executive Officer
313 Park Ave., Ste. 400
Falls Church, VA 22046

Dear Bill:

Carondelet Health Network is a multisystem network of hospitals consisting of two hospitals in Tucson and a third hospital in Nogales along the Mexico border. We have established programs and services to fulfill the health ministry of the Sisters of St. Joseph of Carondelet and to strengthen the Mission of the Roman Catholic Church.

Carondelet Foundation is a not-for-profit entity and operates for and reports to the CEO of Carondelet Health Network. It is very much a part of the above hospitals. We strongly feel that in order to continue serving our community, it is important for Carondelet Foundation to have access to patient names and addresses. It is imperative that the language in the proposed regulations by the Department of Health & Human Services includes hospital fundraisers as part of hospital operations. We have always respected the privacy of our patients and believe strongly in the AHP Standards of Conduct and the donor Bill of Rights. I know that hospitals throughout the country depend on direct mail to past patients in order to acquire donors. Solicitation of former patients introduces us to people who will become regular supporters as donors, volunteers and even trustees. That friendship begins when we receive a positive response to a mail appeal. A lack of response is all it takes to show us we should not mail letters in the future.

Just last month Carondelet Foundation received \$13,765 in donations for the benefit of Carondelet's Hospice program from a *Holiday Tree of Memories* reception held for the families of former patients in the Hospice program. This helps our Hospice and provides a spiritually uplifting and educational opportunity for those families who have lost loved ones. The money raised is used to enhance services such as the 13-month bereavement program for grieving families, which is not reimbursed by Medicare. Our outreach programs will be in jeopardy if we are denied patient demographic information.

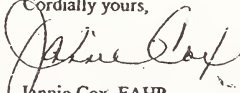
Member of
Carondelet Health
System

Sponsored by the
Sisters of St. Joseph
of Carondelet

LH120 7/99

We encourage you to raise awareness in HHS of our need for access to patient demographic information to enable us to serve our communities. We have a responsibility, we believe, to raise those dollars in the most cost-effective way. The lower our costs, the more funds there are for direct services to patients and their families. Should we send an expensive mailing to our entire community or should we ask our patients, the people we have served, those who may have felt the loving touch of our mission? Also let us keep in mind that anyone can ask to have their name removed from our mailing or database, as we respect the privacy of our patients. As many as 1,500 patients respond favorably each year to our mailings with a gift. These donors do not consider it an invasion of their privacy. Goodwill toward our fellow human beings has been demonstrated, especially in the United States, for centuries by the generosity of Americans everywhere. Let us not erode this basic foundation.

Cordially yours,


Jannie Cox, FAHP
Chief Executive Officer

JCjd



Tel 732-751-5100
Fax 732-751-5120

Affiliated Foundations
4900 Route 33
Suite 200
Neptune, NJ 07753

January 30, 2001

William C. McGinly, Ph.D., CAE
President, Chief Executive Officer
Association for Healthcare Philanthropy
313 Park Avenue, Suite 400
Falls Church, VA 22046

RE: Patient Privacy Regulations

Dear Bill,

I have been so encouraged by your efforts and those of many of our colleagues to assure that our fund raising programs will be able to continue using names of people who have used our hospitals for care. I have been in the hospital fund raising field since 1984...with two systems on the west coast and two systems on the east coast. Each foundation's fund raising programs relied upon those people who have been patients or families of patients.

In 2000 our three foundations - Jersey Shore Medical Center Foundation, Medical Center of Ocean County Foundation and Riverview Foundation - raised more than \$6 million for our hospitals, and with the exception of private foundation support, most of those funds came from people who had been identified over the years through patient lists.

Demographic information only is used for contacting past patients. Confidential information is never looked at or shared with the foundation staffs. We mail to inpatients and outpatients with information about new programs at our hospitals and soliciting financial support for those programs.

Our system provided more than \$60 million in uncompensated care and community outreach programs to the members of our two-county service area. Reimbursements are being continuously reduced, and our hospitals rely more and more on contributions from

members of our communities, most of whom are grateful patients. If it wasn't for these grateful and generous people, it would be more difficult for our hospitals to have positive bottom lines.

Please continue your efforts in getting legislators to understand the importance of philanthropic support and the major role it plays at hospitals throughout our country. I'm sure that once they understand they will continue to allow us access to patient demographic information so that we can continue to build those relationships with those special friends who are appreciative that are hospitals have been there for them.

Thank you.

Sincerely,



Paulette Roberts, CFRE
Executive Director

/PR

Medical Center
of
Ocean County
Foundation

DATE: 1/26/2001
TO: Bill McGinly, President Association for Healthcare Philanthropy
FR: Josephine Capozzi, Director of Development
RE: Privacy

Dear Mr. McGinly,

I want to thank you for your efforts to raise awareness with the Department of Health and Human Services about the need for health care foundations to have access to patient demographic information.

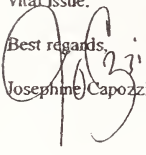
The proposed regulations by the Department of Health and Human Services to protect the privacy of medical records will hurt many hospitals, their foundations, and communities which they serve including the Medical Center of Ocean County (MCOC). The role of MCOC Foundation is to provide an opportunity for donors to fulfill their philanthropic intentions by identifying services offered in their communities.

At MCOC, we are in a position that demands we understand and communicate with our constituency on a regular basis. In May of 2000, we closed one of our two hospitals and reoriented emergency services for our population. Doing this has caused a lot of conflict in the community and education has become a high priority. Utilizing our patients and donors an important message has been sent into the communities we serve -- a message of partnership. We need our patients, their friends, and families to help us provide the very best care possible.

If we were denied access to patient demographic information a large portion of our educational and fundraising efforts would be lost. This loss would affect the hospital financially, as a large portion of our outreach into the community would be jeopardized. A significant percentage of new donors come from our grateful patients. We have always respected the privacy of our patients and believe strongly in the AHP Standards of Conduct and the Donor Bill of Rights.

In 2000, I received my CFRE accreditation through AHP and in many ways it was a confirmation of my personal belief in the AHP Standards of Conduct and the Donor Bill of Rights. I am a believer -- please continue your important efforts to inform HHS of this vital issue.

Best regards,


Josephine Capozzi, CFRE

JERSEY SHORE MEDICAL CENTER FOUNDATION

P.O. BOX 1064 • NEPTUNE, NJ 07753-4470

(NJ) 751-5117 • FAX (732) 751-5120

January 30, 2001

William C. McGinly, Ph.D., CAE
AHP
313 Park Avenue, Suite 400
Falls Church, VA 22046

Dear Bill:

Thank you for your efforts to raise awareness with the Department of Health and Human Services about the need for health care fund raisers to have access to patient demographic information. It is now important that we make sure the Bush administration is educated also.

Jersey Shore Medical Center is a 502-bed acute care hospital located in central Monmouth County. A major teaching hospital and tertiary care center, Jersey Shore offers the only Level II Regional Trauma Center and Pediatric Trauma Center. JSMC is a Level III Regional Perinatal Center and Neonatal Intensive Care Unit, A regional Pediatric Intensive Care Unit, and has the only open-heart surgery program in the two-county area. We also offer a single-room maternity unit, ambulatory care, and behavioral health services. JSMC's Cancer Center offers stem-cell transplant, a linear accelerator and the latest developments in cancer prevention and treatment. JSMC's Family Health Center conducts 20,000 visits annually most of which are for noninsured patients.

Jersey Shore Medical Center Foundation provided \$1.5 million dollars to Jersey Shore Medical Center last year in support of programs, services and equipment. Without this funding, many of these programs, services and equipment would not have been available to the community we serve. This funding provided medication for low income AIDS and family health center patients, support groups for cancer patients and their loved ones, equipment for our Inpatient Hospice Unit, developmental kits for our neonatal intensive care unit, a New Health Sciences Library that is open to the community, a Multi Slice CT Scanner, among other services.

We rely heavily on support from individuals to help ease the tremendous pressure of declining reimbursements for health care services provided by our medical center. The majority of our revenue comes from patients and former patients. A significant percentage of new donors comes from our

grateful patients. If we were denied access to patient demography information, Jersey Shore Medical Center's ability to provide the community with the service it deserves would be placed in jeopardy.

We have always respected the privacy of our patients and believe strongly in the AHP Standards of Conduct and the Donor Bill of Rights.

Please continue in your efforts in getting regulators to understand the important role philanthropy plays in the provision of quality health care in this country.

Sincerely,



June E. Lynch CFRE
Director of Development



Henry Mayo

Newhall Memorial Health Foundation

23845 McBean Parkway Valencia California 91355-2083 Telephone (661) 253-8082

January 15, 2000

William C. McGinly, Ph.D., CAE
President and Chief Executive Officer
Association for Healthcare Philanthropy
313 Park Avenue, Suite 400
Falls Church, VA 22046

Dear Bill:

We are extremely pleased with the findings of the Health and Human Services (HHS) decision to include healthcare philanthropy and fundraising as the definition of health care operations. Because hospital foundations are a viable part of healthcare operations and depended upon to fund state-of-the-art equipment, new services and build new facilities, the importance of continued fundraising capabilities is extremely important for the progression of non-profit healthcare organizations.

Henry Mayo Newhall Memorial Hospital (HMNMH), a 227-bed non-profit community hospital in Southern California - just 40 miles north of Los Angeles, has relied on the fundraising efforts of the Henry Mayo Newhall Memorial Health Foundation to build new facilities with the help of our community which includes corporations, organizations, and individuals - many of whom are or have been patients.

Due to the current economic climate in the healthcare industry, any excess of revenue over operating expense is virtually non-existent. Over the next five years, hospitals will absorb a significant decrease in Medicare reimbursements, as mandated by the Federal Balanced Budget Act approved by Congress and President Clinton. An additional financial complication includes the cost to repair California hospital facilities per SB1953 resulting from the 1994 Northridge earthquake. Because of these types of financial constraints, hospitals rely heavily on the philanthropic support generated by hospital foundations to purchase vitally needed capital equipment and to expand services.

I believe that without the ongoing philanthropic endeavors of healthcare fundraising and the tools necessary to encourage support, hospitals will be unable to cope with ever-increasing financial challenges now and in the future.

Sincerely,


 Lisa Foust, FAHP
 President

10/1/99
 here

HEALTH PRIVACY PROJECT

INSTITUTE FOR HEALTH CARE
 RESEARCH AND POLICY
 GEORGETOWN UNIVERSITY

Overview of HIPAA Privacy Regulation

Currently, there is no comprehensive federal law that protects the privacy of people's medical records. The 1996 Health Insurance Portability and Accountability Act (HIPAA) included legislative/regulatory deadlines in order to fill this significant gap in federal rules. HIPAA provides that if Congress failed to pass a comprehensive health privacy law by August 21, 1999, the Secretary of Health and Human Services is required to issue health privacy regulations.

Despite the introduction of numerous bills, and many hearings over the past three years, Congress failed to pass health privacy legislation and thus triggered the regulatory deadline. On October 29, 1999, the Clinton Administration issued its draft regulations. By the close of the public comment period, the Administration had received over 52,000 comments, more than half of them from consumers and consumer advocates.

The final regulations were released on December 20, 2000. The regulations will become effective 60 days after they are published in the Federal Register. There is a two-year implementation period before compliance with the regulation is required.

A copy of the regulation is available at: <http://aspe.hhs.gov/admsimp/>.

The following chart summarizes key provisions of the final regulation and provides Health Privacy Project commentary.

2233 Wisconsin Avenue, NW Suite 525 Washington, DC 20007
 phone 202.687.0880 fax 202.784.1265
www.healthprivacy.org

Topic	The Final Regulation	Health Privacy Project Comments
Who's Covered	Covered entities include: ◆ <i>Health Plans</i> HMOs, health insurers, group health plans including employee welfare benefit plans ◆ <i>Health Care Clearinghouses</i> Persons and organizations that translate health information to or from the standard format that will be required for electronic transactions under HIPAA ◆ <i>Certain Health Care Providers</i> Those who use computers to transmit health claims information	Under HIPAA, the Secretary only has the authority to cover these three entities. The regulation, therefore, does not directly apply to many other entities that collect and maintain health information such as employers, life insurers, researchers, and public health officials. <i>Only Congress can fill these critical gaps.</i>
What's Covered	Only the use and disclosure of "protected health information" is covered. In order to be considered "protected health information" under the regulation, information must: ◆ Relate to a person's physical or mental health, the provision of health care, or the payment of health care; ◆ Identify, or could be used to identify, the person who is the subject of the information; and ◆ Be created or received by a covered entity. Such information is protected regardless of the format in which it is transmitted or maintained—oral, electronic or paper.	There is some dispute over whether the Secretary has the authority to cover health information that is in any format other than electronic. Practically speaking, covering health information that is maintained or transmitted in any medium or format is a sensible move. Limiting coverage to electronically transmitted data would be impractical, unenforceable and would deter covered entities from moving towards electronic health data systems. Even with this improvement, the regulation still fails to cover a large portion of health care information due to statutory limits on the Secretary's authority; namely, identifiable health information generated by entities not covered by the regulation such as employers or life insurers. <i>Only Congress can fill in these critical</i>

Topic	The Final Regulation	Health Privacy Project Comments
What's Covered (continued)	There are incentives for covered entities to create and use " <i>de-identified information</i> ," health information which has been stripped of elements that could be used to identify individual subjects.	gaps. Encouraging the use of information that does not identify the patient helps ensure that people's privacy can be maintained to the maximum extent possible.
Patient Access	◆ Individuals have a right to see and copy their own health information, including documentation of to whom the information has been disclosed. ◆ Individuals are given the right to request amendment or correction of health information that is incorrect or incomplete. ◆ There are limited exceptions to when patients can access their own information such as when such access would endanger the life or safety of any individual.	Currently, there is no federal law granting persons the right to obtain their medical records. Although the majority of states provide patients the right of access to <i>some</i> of their medical records, very few do so in a comprehensive fashion. In fact, some states have <i>no</i> such statutory right of access. The final regulation, therefore, establishes a significant, new legal right for individuals to see and copy their own health information.
Notice	Health plans and health care providers are required to provide written notice of their privacy practices, including a description of an individual's rights with respect to protected health information (such as the right to inspect and copy health records) and the anticipated uses and disclosures of this information that may be made without the patient's written authorization.	We are pleased that this basic fair information has been adopted in the regulation.

Topic	The Final Regulation	Health Privacy Project Comments
General Rule- Patient permission required	◆ An individual's written permission is required for all uses or disclosures not permitted or required under the privacy regulation. ◆ The regulation uses two different types of written permission: 1. Consents—used for treatment, payment and health care operations; and 2. Authorizations—used for other purposes.	The regulation permits uses and disclosures <i>without</i> authorization or consent for <i>many</i> purposes. The distinction between consents and authorizations is somewhat confusing. Consents and authorizations are discussed separately below.
Treatment, Payment, and Health Care Operations (Consents)	◆ Covered health care providers <i>must</i> generally obtain the patient's consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations. ◆ Providers <i>may condition</i> treatment on patient's providing consent form. ◆ Health plans and health care clearinghouses <i>may</i> obtain such consent for their own use or disclosure to carry out these purposes. ◆ Health plans <i>may condition</i> enrollment on provision of consent. ◆ Individuals have a <i>right to request restrictions</i> on how health information is used or	We believe that obtaining consent before the use or disclosure of health information is a fundamental component of fair information practices. As such, we support the new consent requirement. We are concerned that a consent for treatment will allow uses and disclosures well beyond what the average health consumer would anticipate. Most people would expect that they are consenting only to the use of health information for <i>their own</i> treatment. However, under the regulation, such a consent would also permit the provider to use and disclose one patient's health information for the treatment of <i>other</i> patients. The right to request a restriction affords individuals with especially sensitive medical conditions an additional

Topic	The Final Regulation	Health Privacy Project Comments
Treatment, Payment, and Health Care Operations (continued)	disclosed for treatment, payment or health care operations purposes.	opportunity to exercise control over their health information. This right should be strengthened.
Authorizations	◆ Authorizations are used for purposes other than treatment, payment and health care operations when use or disclosure is not otherwise permitted under the regulation. ◆ Providers generally <i>may not</i> condition treatment on authorization. ◆ Health plans <i>may</i> condition enrollment, eligibility and payment on authorization permitting disclosure and use related to these purposes. Psychotherapy notes are an exception.	Patient authorization is critical to protecting patient privacy. Authorizations provide individuals with some degree of control over what information about them is disclosed, to whom, and for what purposes.
Patient Permission <i>Not Required</i>	Health information may be disclosed for a number of purposes without any patient authorization or consent including, but not limited to: public health activities, research, and fraud investigations.	See our comments on law enforcement and research.
Business Associates	◆ Business associates are persons who perform functions or activities involving the use or disclosure of protected health information for or on behalf of a covered entity. ◆ A written contract is necessary in order for a business associate to receive information from, or	This requirement indirectly expands the scope of the privacy regulation. Wrongful disclosures that violate business partner contracts may be subject to lawsuits brought by the

Topic	The Final Regulation	Health Privacy Project Comments
Business Associates (continued)	on behalf of, a covered entity. Under the contract, the business associate is essentially bound to the use and disclosure limitations of the regulation.	individual under state contract law. Although we support this indirect regulation of secondary users of health information, we would prefer that these entities be directly regulated. <i>Only Congress can remedy this situation.</i>
Minimum Necessary	Covered entities must make reasonable efforts to limit protected health information to the <i>minimum amount necessary</i> to accomplish the intended purpose of the use, disclosure or request for health information from another. This standard <i>does not</i> apply to disclosures for treatment and other specified purposes.	The minimum necessary standard imposes an important limitation on the amount of health information disclosed. However, we believe the standard should apply to a broader category of disclosures, including those made for treatment.
Directory Assistance and Next of Kin	For providing information to a <i>directory</i> (such as a hospital's patient directory) or to <i>next of kin</i> or other persons involved in the care of the patient, the patient must be given <i>notice</i> and the opportunity to <i>opt out before</i> the information is disclosed.	An <i>opt in</i> procedure, where privacy is protected unless the patient agrees to the disclosure, would be preferable.
Psychotherapy Notes	♦ There are stricter requirements than for other health information. Written authorization is required for most uses or disclosures. ♦ Health plans may not condition enrollment or eligibility for benefits on the patient's providing an authorization for the use and disclosure of	Psychotherapy notes differ considerably from other kinds of information in a patient's medical record. Such notes are highly subjective and sensitive, and should not be made available beyond the treating provider without the patient's consent. Notes of psychotherapy sessions are not necessary for health plans to make enrollment, eligibility and payment

Topic	The Final Regulation	Health Privacy Project Comments
Psychotherapy Notes (continued)	psychotherapy notes.	decisions. The approach taken by the regulation is reasonable— it allows health plans to condition these services on the patient's authorizing the disclosure of treatment times, general diagnosis and other general information but prohibits plans from requiring access to detailed session notes.
Minors' Rights	Unemancipated minor has sole right to exercise rights under regulation including: ♦ Minor has consented to health care service and no other ♦ consent to such health care is required by law; or ♦ Parent or guardian assents to an agreement of confidentiality.	Under this provision, the federal privacy right will attach to the right to consent to treatment. Other law, including state law, will govern when a minor may consent to treatment without adult involvement. Parental notification laws are not affected by the federal regulation.
Law Enforcement	Covered entities are permitted to disclose protected health information to law enforcement officials: ♦ Pursuant to warrant, subpoena, or order issued by a judicial officer; ♦ Pursuant to a grand jury subpoena; or ♦ Pursuant to an administrative subpoena or summons, civil investigative demand or similar certification where a three-part test is met: the information is relevant, the request is specific, and de-identified information could not reasonably be used.	The regulation falls far short of the standards established in most federal privacy laws. Only the first category requires any independent judicial review. Administrative summons and subpoenas may be issued by the investigating authority <i>with no independent review</i> by a neutral magistrate to determine whether the request should be granted or denied.

Topic	The Final Regulation	Health Privacy Project Comments
Law Enforcement (continued)	The regulation also permits additional disclosures without any written request.	
Research	Covered entities can disclose protected health information without a patient's authorization only to researchers whose protocol has been reviewed and approved by an Institutional Review Board (IRB) or a "privacy board." The regulation includes new evaluation criteria for all waivers of informed consent. Information can only be released to researchers if it meets the criteria.	Currently, only research <i>that receives federal funding</i> is subject to the "Common Rule," a federal regulation that requires that any use of identifiable private information be overseen by an Institutional Review Board (IRB). The final privacy regulation takes an important step forward by extending the Common Rule's requirements for a waiver of informed consent to <i>all researchers</i> , including privately funded researchers.
Enforcement	HIPAA grants the Secretary the authority to impose civil monetary penalties against covered entities that fail to comply and criminal penalties for certain wrongful disclosures of protected health information. ♦ The civil fines are capped at \$25,000 for each calendar year for each provision that is violated. ♦ The criminal penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain. The maximum is 10 years in prison and a \$250,000 penalty ♦ The Secretary will, to the extent practicable, seek the	Of concern is that HIPAA does not provide for a private right of action for individuals, which would allow individuals to sue for violations of their rights. The Administration is on record supporting a private right of action in pending legislation. <i>Only Congress, however, can give people a right to this critical enforcement mechanism.</i>

Topic	The Final Regulation	Health Privacy Project Comments
Enforcement (continued)	cooperation of covered entities in obtaining compliance. Any person who believes that a covered entity is not complying with the regulatory requirements may file a complaint with the Secretary.	
Preemption	HIPAA provides that state laws that are more protective of individual privacy will stand. States are also free to pass stronger laws in the future.	Leaving stronger state laws in place is critical. Although most states do not have comprehensive health privacy laws, many states do have detailed, stringent standards for certain information, such as mental health, genetic testing, and HIV/AIDS. These stronger privacy protections would remain in force.

The CHAIRMAN. Thank you very much, the hearing is adjourned.
[Whereupon, at 12:10 p.m., the committee was adjourned.]

○

CMS Library

C2-07-13

7500 Security Blvd.

Baltimore, Maryland 21244

CMS LIBRARY



3 8095 00006698 1

Form with faint, illegible text and a rectangular border.